



ISO 20000 INTERNAL AUDITOR/LEAD AUDITOR PROFESSIONAL CERTIFICATION



I20000IA/LA™ Versión 092020

...

ISO 20000 INTERNAL AUDITOR / LEAD AUDITOR I20000IA/LA



I20000IA/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.

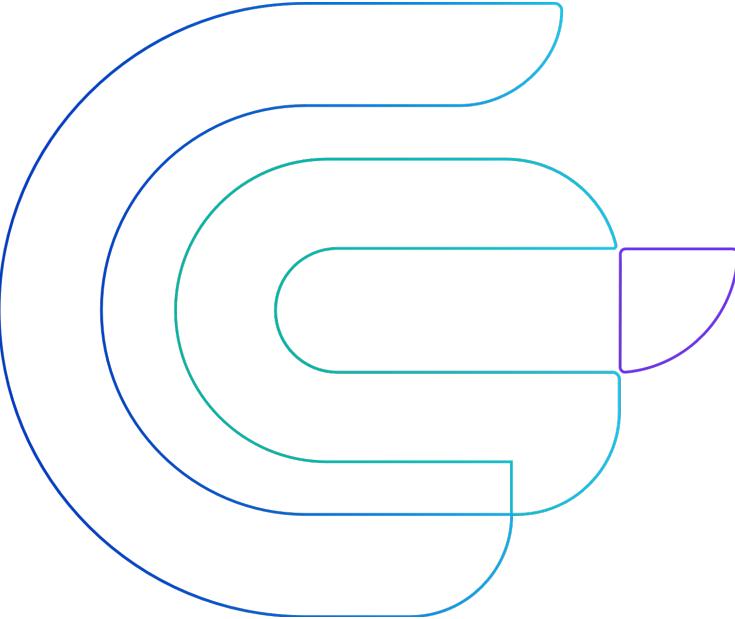


¿Por qué son importantes?



- **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.





Certiprof ISO/IEC 20000 Internal Auditor - I20000IA™

Issued by [Certiprof](#)

Holders of this certification have demonstrated an understanding of the scope, purpose, objectives and requirements of ISO/IEC 20000 and how they should be used during an audit process. They understand the principles of IT Service Management and the ability to explain advise on findings related to the applicability of the standard.

[Learn more](#)

[Earn this Badge](#)

Certification

Paid

Skills

- [Auditing](#)
- [Compliance](#)
- [Continual Improvement](#)
- [ISO 20000](#)
- [IT Management](#)
- [Service Management](#)
- [SMS](#)

<https://www.credly.com/org/certiprof/badge/certiprof-iso-iec-20000-internal-auditor-i20000ia>





The badge is circular with a blue and gold border. The top arc contains the text "PROFESSIONAL CERTIFICATION". The center features a blue "C" logo above the word "certiprof" in white, with a registered trademark symbol. Below that is a dark blue banner with the text "ISO 20000 LEAD AUDITOR". A small white tab on the right side contains the text "I20000LA™".

[Earn this Badge](#)

[Learn more](#)

 Certification  Paid

Skills

Auditing Compliance Continual Improvement ISO 20000 IT Management
Service Management SMS

Certified ISO/IEC 20000 Lead Auditor - I20000LA™

Issued by [Certiprof](#)

Holders of this certification have demonstrated an understanding of the scope, purpose, objectives and requirements of ISO/IEC 20000 and how they should be used during an audit process. They understand the principles of IT Service Management and developed skills to perform the audit process and know the responsibilities of being a lead auditor and understand how to develop an SMS.

<https://www.credly.com/org/certiprof/badge/certified-iso-iec-20000-lead-auditor-i20000la>



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

#I20000IA/LA #certiprof



 certiprof®

•••

• • •

Agenda



I20000IA/LA™ Versión 092020



Agenda

Fundamentos de la Norma ISO

20000-1

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

Módulo de Auditor 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. Disponible para candidatos a examen de auditor y/o auditor líder.*



...

1. Introducción y Antecedentes



Introducción

- ISO/IEC 20000-1.
- Historia de la Norma.
- Estado actual.



Introducción

- La Norma ha sido diseñada para ***"para especificar los requisitos para el establecimiento, la implementación, el mantenimiento y la mejora continua de un sistema de gestión de servicios (SGS)".***
- Esta norma es intencionadamente independiente de guías específicas. La organización puede utilizar una combinación de marcos generalmente aceptados junto a su propia experiencia. Los requisitos especificados en este documento están alineados con metodologías de mejora comúnmente utilizadas.
- Para prestar soporte al SGS pueden utilizarse herramientas adecuadas para la gestión de servicios.



Historia de la Norma

En el año 1989 la entidad británica BSI comenzó la definición de un estándar para la gestión de servicio TI, que finalizó con su publicación como estándar BS 15000 en 1995.

A partir de este año BSI continuó con el desarrollo del estándar elaborando una segunda parte con el objetivo de profundizar en los conceptos de la parte 1.

En el año 2000 es publicada la Norma BS 15000 parte 1 y 2.

En diciembre del 2005 se publicó la Norma ISO/IEC 20000 partes 1 y 2.

En el año 2011 se actualiza a la versión de Normas ISO/IEC 20000:2011.

Finalmente 2018 se publica la ISO/IEC 20000:2018 adoptando la estructura común de alto nivel para normas de sistemas de gestión (Anexo SL).



Cambios Realizados en la Norma ISO/IEC 20000-1

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

- a) Se ha reestructurado de acuerdo a la estructura de alto nivel utilizada para todas las normas de sistema de gestión (de acuerdo con el anexo SL del Suplemento ISO Consolidado a las Directivas ISO/IEC Parte 1). Esto ha introducido nuevos requisitos comunes para el contexto de la organización, la planificación para alcanzar objetivos y las acciones para abordar los riesgos y las oportunidades. Existen algunos requisitos comunes que han actualizado requisitos previos, por ejemplo, información documentada, recursos, competencia y concienciación.
- b) Se han tenido en cuenta las tendencias emergentes en la gestión de servicios, incluidos temas como la comoditización de los servicios, la gestión de múltiples proveedores por parte de un integrador de servicios interno o externo y la necesidad de determinar el valor de los servicios para los clientes.



Cambios Realizados en la Norma ISO/IEC 20000-1

- c) Se han eliminado algunos detalles para concentrarse en qué hacer y dejar a las organizaciones la libertad de cómo cumplir los requisitos.
- d) Se han incluido nuevas características como nuevos requisitos de conocimiento y planificación de los servicios.
- e) Se han separado los apartados que se combinaron previamente para los procesos de gestión de incidencias, de peticiones de servicio, de la continuidad de servicio, de la disponibilidad de servicio, de niveles de servicio, de catálogo de servicios, de la capacidad y de la demanda.
- f) Se ha cambiado el nombre de "Gobierno de los procesos operados por terceros" a "Control de partes involucradas en el ciclo de vida de los servicios" y se han actualizado los requisitos para hacer referencia tanto a servicios y componentes de servicios como a procesos. Se ha puntualizado que la organización no puede demostrar conformidad con los requisitos especificados en este documento si se utilizan terceros para proporcionar u operar todos los servicios, componentes de servicios o procesos dentro del alcance del sistema de gestión de servicios (SGS).



Cambios Realizados en la Norma ISO/IEC 20000-1

- g) Se ha separado el capítulo 3 (Términos y definiciones) en apartados para los términos de los sistemas de gestión y para los términos de la gestión de servicios. Se han llevado a cabo muchos cambios en las definiciones. Los cambios fundamentales incluyen:
1. Se han agregado algunos términos nuevos para el anexo SL, como "objetivo" o "política", y se han agregado algunos específicos para gestión de servicios, como "activo" o "usuario";
 2. El término "proveedor de servicios" ha sido reemplazado por "organización" para ajustarse al texto común del anexo SL;
 3. El término "grupo interno" ha sido reemplazado por "proveedor interno" y el término "suministrador" ha sido reemplazado por "proveedor externo";
 4. La definición de "seguridad de la información" se ha alineado con la Norma ISO/IEC 27000. Además, el término "disponibilidad" ha sido sustituido por "disponibilidad de servicio" para diferenciarlo del término "disponibilidad" que ahora se utiliza en la definición revisada de "seguridad de la información".



Cambios Realizados en la Norma ISO/IEC 20000-1

- h) Se ha minimizado la información documentada requerida, dejando solo documentos clave, como el plan de gestión de servicios. Otros cambios de información documentada son:
1. Se ha eliminado el requisito relativo al plan documentado de capacidad y se han reemplazado por un requisito de planificación de la capacidad.
 2. Se ha eliminado el requisito relativo al plan de disponibilidad documentado y se ha reemplazado el requisito de documentar los requisitos y objetivos de disponibilidad.
 3. Se ha eliminado el requisito de una base de datos de gestión de la configuración y se ha reemplazado por requisitos y objetivos de información de la configuración.
 4. Se ha eliminado el requisito de una política de entregas y se ha reemplazado por un requisito para definir tipos y frecuencia de las entregas.
 5. Se ha eliminado el requisito de una política de mejora continua y se ha reemplazado por un requisito para definir los criterios de evaluación de oportunidades de mejora.



Cambios Realizados en la Norma ISO/IEC 20000-1

- i) Se han actualizado y renumerado las figuras 2 y 3 como figuras 1 y 2. Se ha eliminado la figura 1 y las referencias al ciclo Planificar-Hacer-Verificar-Actuar (o Plan-Do-Check-Act) ya que no es específicamente utilizado en el anexo SL, puesto que se pueden utilizar muchos métodos de mejora con las normas de sistemas de gestión.
- j) Se han trasladado los requisitos de informes detallados desde el apartado de informes de servicio a los apartados donde es probable que se generen los informes.



Cambios Realizados en la Norma ISO/IEC 20000-1

ISO/IEC 20000:2018	ISO/IEC 20000:2011
4. Contexto de la organización.	4.1 Responsabilidades de la dirección. 4.5.1 Definir el alcance. 4.5.2 Planificar el SGS (Planificar). 7.1 Gestión de las relaciones del negocio.
4.1 Comprensión de la organización y su contexto.	Nuevo
4.2 Comprensión de las necesidades y expectativas de las partes interesadas.	4.1.4 Representante de la dirección. 7.1 Gestión de las relaciones del negocio.
4.3 Determinación del alcance del sistema de gestión de servicios.	4.5.1 Definir el alcance.
4.4 Sistema de gestión de servicios.	4.1.1 Compromiso con la dirección. 4.5.3 Implementar y operar el SGS (Hacer).
5. Liderazgo.	4.1 Responsabilidades de la dirección.
5.1 Liderazgo y compromiso.	4.1.1 Compromiso con la dirección.
5.2 Política.	4.1.2 Política de gestión de servicio.
5.2.1 Establecer la política de gestión de servicios.	4.1.2 Política de gestión de servicio.
5.2.2 Comunicar la política de gestión de servicios.	4.1.2 Política de gestión de servicio.
5.3 Roles, responsabilidades y autoridades en la organización.	4.1.3 Autoridad, responsabilidad y comunicación. 4.1.4 Representante de la dirección.



ISO/IEC 20000:2018	ISO/IEC 20000: 2011
6. Planificación.	4.1.1 Compromiso con la dirección. 4.5.2 Planificar el SGS (Planificar). 6.6.1 Política de seguridad de la información.
6.1 Acciones para tratar riesgos y oportunidades.	4.1.1 Compromiso con la dirección. 4.5.2 Planificar el SGS (Planificar). 6.6.1 Política de seguridad de la información.
6.2 Objetivos de gestión de servicios y planificación para su consecución.	4.1.1 Compromiso con la dirección.
6.2.1 Establecer objetivos.	4.1.1 Compromiso con la dirección.
6.2.2 Planificar la consecución de los objetivos.	Nuevo.
6.3 Planificar el sistema de gestión de servicios.	4.5.2 Planificar el SGS (Planificar).



ISO/IEC 20000:2018	ISO/IEC 20000: 2011
7. Apoyo.	4.1 Responsabilidades con la dirección. 4.3 Gestión de la documentación. 4.4 Gestión de los recursos.
7.1 Recursos.	4.4.1 Provisión de los recursos.
7.2 Competencia.	4.4.2 Recursos humanos.
7.3 Concienciación	4.1.1 Compromiso con la dirección. 4.1.2 Política de gestión de servicio. 4.4.2 Recursos humanos.
7.4 Comunicación.	4.1.3 Autoridad, responsabilidad y comunicación.
7.5 Información Documentada.	4.3 Gestión de la documentación.
7.5.1 Generalidades.	4.3.1 Establecer y mantener los documentos.
7.5.2 Creación y actualización de la información documentada.	4.3.2 Control de los documentos.
7.5.3 Control de la información documentada.	4.3.2 Control de los documentos. 4.3.3 Control de los registros.
7.6 Conocimiento	Nuevo.



	4. Requisitos generales del sistema de gestión de servicio.
	5. Diseño y transición de servicios nuevos o modificados.
	6. Proceso de entrega del servicio.
	7. Procesos de las relaciones.
	8. Procesos de resolución
	9. Procesos de control.
8. Operación.	
8.1 Planificación y control operacional.	4.1.4 Representante de la dirección. 4.2 Gobierno de procesos operados por otras partes. 4.5.3 Implementar y operar el SGS (Hacer). 9.2 Gestión del cambio.
8.2 Portafolio de servicios.	4.1.4 Representante de la dirección. 4.2 Gobierno de procesos operados por otras partes. 4.5.3 Implementar y operar el SGS (Hacer). 5.2 Planificación de servicios nuevos o modificados. 6.1 Gestión de nivel de servicio. 9.1 Gestión de la configuración.
8.2.1 Prestación de servicios.	4.5.3 Implementar y operar el SGS (Hacer).
8.2.2 Planificación de servicios.	4.1.4 Representante de la dirección. 5.2 Planificación de servicios nuevos o modificados.
8.2.3 Control de partes involucradas en el ciclo de vida de los servicios.	4.2 Gobierno de procesos operados por otras partes. 5.2 Planificación de servicios nuevos o modificados.
8.2.4 Gestión de catálogo de servicios.	6.1 Gestión de nivel de servicio.
8.2.5 Gestión de activos.	4.1.4 Representante de la dirección.
8.2.6 Gestión de la configuración.	9.1 Gestión de configuración.



ISO/IEC 20000:2018	ISO/IEC 20000:2011
8.3 Relación y acuerdo.	6.1 Gestión del nivel de servicio. 6.2 Reporte del servicio. 7. Procesos de las relaciones.
8.3.1 Generalidades.	7.2 Gestión de los suministradores.
8.3.2 Gestión de las relaciones con el negocio.	6.2 Reporte del servicio. 7.1 Gestión de las relaciones del negocio.
8.3.3 Gestión de los niveles de servicio.	6.1 Gestión del nivel de servicio. 6.2 Reporte del servicio.
8.3.4 Gestión de proveedores.	6.1 Gestión del nivel de servicio. 7.2 Gestión de los suministradores.
8.3.4.1 Gestión de proveedores externos.	7.2 Gestión de los suministradores.
8.3.4.2 Gestión de proveedores internos y clientes actuando como proveedores.	6.1 Gestión del nivel de servicio.
8.4 Oferta y demanda.	6.4 Presupuesto y contabilidad de los servicios. 6.5 Gestión de la capacidad.
8.4.1 Presupuesto y contabilidad de servicios.	6.4 Presupuesto y contabilidad de los servicios.
8.4.2 Gestión de la demanda.	6.5 Gestión de la capacidad.
8.4.3 Gestión de la capacidad.	6.5 Gestión de la capacidad.
8.5 Producción y provisión del servicio.	5. Diseño y transición de servicios nuevos o modificados. 9. Procesos de control.



ISO/IEC 20000:2018	ISO/IEC 20000:2011
8.5.1 Gestión de cambios.	5.1 Generalidades. 6.3 Gestión de la continuidad y disponibilidad del servicio. 6.6 Gestión de la seguridad de la información. 9.2 Gestión del cambio.
8.5.1.1 Políticas de gestión de cambios.	9.2 Gestión del cambio.
8.5.1.2 Inicio de la gestión de cambios.	5.1 Generalidades. 9.2 Gestión del cambio.
8.5.1.3 Actividades de gestión de cambios.	6.3.2 Planes de continuidad y disponibilidad del servicio. 6.3.3 Monitoreo y pruebas de la continuidad y disponibilidad del servicio. 9.2 Gestión del cambio. 9.3 Gestión del release y despliegue.
8.5.2 Diseño y transición de servicios.	5. Diseño y transición de servicios nuevos o modificados. 6.2 Reporte del servicio.
8.5.2.1 Planificación de servicios nuevos o modificados.	5.2 Planificación de servicios nuevos o modificados.
8.5.2.2 Diseño.	5.3 Diseño y desarrollo de servicios nuevos o modificados.
8.5.2.3 Construcción y transición.	5.3 Diseño y desarrollo de servicios nuevos o modificados. 5.4 Transición de los servicios nuevos o modificados. 6.2 Reporte del servicio.
8.5.3 Gestión de entregas y despliegues.	9.1 Gestión de configuración 9.3 Gestión del release y despliegue.



ISO/IEC 20000:2018	ISO/IEC 20000:2011
8.6 Resolución y ejecución.	8.1 Gestión de incidentes y solicitudes de servicio. 8.2 Gestión del problema.
8.6.1 Gestión de incidencias.	6.2 Reporte de servicio. 8.2 Gestión del problema.
8.6.2 Gestión de peticiones de servicio.	8.1 Gestión de incidentes y solicitudes de servicio.
8.6.3 Gestión de problemas.	8.2 Gestión del problema.
8.7 Aseguramiento de servicios.	6.3 Gestión de la continuidad y disponibilidad del servicio. 6.6 Gestión de la seguridad de la información.
8.7.1 Gestión de la disponibilidad de servicios.	6.3 Gestión de la continuidad y disponibilidad del servicio.
8.7.2 Gestión de la continuidad de los servicios.	6.2 Reporte de servicio. 6.3 Gestión de la continuidad y disponibilidad del servicio.
8.7.3 Gestión de la seguridad de la información.	6.6 Gestión de la seguridad de la información.
8.7.3.1 Política de seguridad de la información.	6.6.1 Política de seguridad de la información.
8.7.3.2 Controles de seguridad de la información.	6.6.2 Controles de seguridad de la información.
8.7.3.3 Incidencias de seguridad de la información.	6.6.3 Cambios e incidentes de seguridad de la información.



ISO/IEC 20000:2018	ISO/IEC 20000:2011
9. Evaluación del desempeño.	4.5.4 Monitorear y revisar el SGS (Verificar). 6.2 Reporte del servicio.
9.1 Monitorización, medición, análisis y evaluación.	4.5.4.1 Generalidades.
9.2 Auditoría Interna.	4.5.4.1 Generalidades. 4.5.4.2 Auditoría interna. 6.2 Reporte del servicio.
9.3 Revisión por la dirección.	4.5.4.1 Generalidades. 4.5.4.3 Revisión de la alta dirección.
9.4 Informes de servicio.	6.2 Reporte del servicio.
10. Mejora.	4.5.5 Mantener y mejorar el SGS (Actuar).
10.1 No conformidad y acción correctiva.	4.5.4.2 Auditoría interna. 4.5.5.1 Generalidades. 6.2 Reporte del servicio.
10.2 Mejora continua.	4.5.5.1 Generalidades. 4.5.5.2 Gestión de mejoras.



...

2. ¿Qué es un SGS?



Sistema de Gestión de Servicios (SGS)

- Un SGS presta ***soporte a la gestión del ciclo de vida de los servicios***, incluyendo la planificación, el diseño, la transición, la entrega y la mejora de los servicios, que cumplen con los requisitos acordados y ofrecen valor para los clientes, los usuarios y la organización que presta los servicios.
- La adopción de un SGS es una decisión estratégica para una organización y está condicionada por los objetivos de la misma, el órgano de gobierno, otras partes implicadas en el ciclo de vida de los servicios y la necesidad de unos servicios eficaces y resilientes.
- La implementación y operación de un SGS proporciona visibilidad continua, control de los servicios y mejora continua, generando una mayor eficacia y eficiencia. La mejora de la gestión de servicios se aplica al SGS y a los servicios.



...

3. Términos y Definiciones (Ver anexo))



• •

Estructura de la Norma



I20000IA/LA™ Versión 092020



Estructura de ISO/IEC 20000-1

- Introducción
 - 1. Objeto y campo de aplicación.
 - 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.
- Apéndice.
- Bibliografía.



Estructura de ISO/IEC 200001

C clientes
(internos y
externos)

Requisitos de los servicios

Servicios

Sistema de Gestión de Servicios (SGS)

Contexto de la Organización

- La organización y su contexto
- Partes interesadas
- Alcance del SGS
- Establecer el SGS

Liderazgo

- Liderazgo y compromiso
- Política
- Roles, responsabilidades y autoridades

Planificación

- Riesgos y oportunidades
- Objetivos
- Plan del SGS

Soporte al SGS

- Recursos
- Competencia
- Concienciación
- Comunicación
- Información documentada
- Conocimiento

Operación del SGS

PLANIFICACIÓN Y CONTROL OPERACIONAL

PORAFOLIO DE SERVICIOS

- Prestación de servicios.
- Planificación de servicios.
- Control de partes involucradas en el ciclo de vida de los servicios.
- Gestión de catálogo de servicios.
- Gestión de activos.
- Gestión de la configuración.

RELACIÓN Y ACUERDO

- Gestión de relaciones con el negocio.
- Gestión de proveedores.

OFERTA Y DEMANDA

- Presupuesto y contabilidad de servicios.
- Gestión de la demanda.
- Gestión de la capacidad.

DISEÑO, CONSTRUCCIÓN Y TRANSICIÓN DE SERVICIOS

- Gestión de cambios.
- Diseño y transición de servicios.
- Gestión de entregas y despliegues.

RESOLUCIÓN Y EJECUCIÓN

- Gestión de incidencias.
- Gestión de peticiones de servicio.
- Gestión de problemas.

ASEGURAMIENTO DE SERVICIOS

- Gestión de la disponibilidad de servicios.
- Gestión de la continuidad de servicios.

EVALUACIÓN DEL DESEMPEÑO

- Monitorización, medición, análisis y evaluación.
- Auditoría interna.
- Informes de servicio.
- Revisión por la dirección.

MEJORA

- No conformidad y acción correctiva.
- Mejora continua.

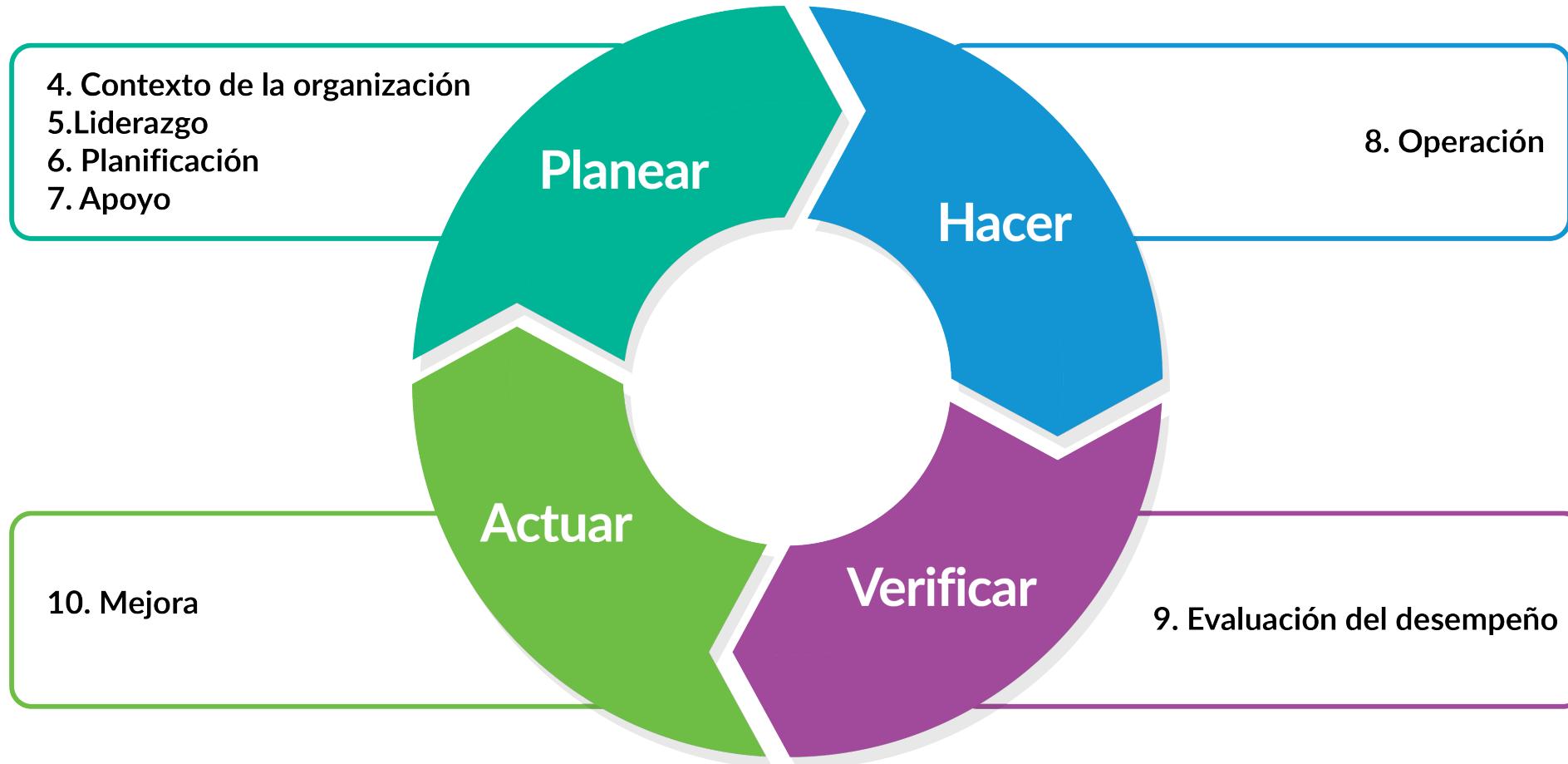
Figura 1: Sistema de Gestión de Servicios.

©ISO. Este material ha sido reproducido de ISO/IEC 20000-1:2018, con permiso del American National Standards Institute (ANSI) en nombre de la Organización Internacional de Normalización. Todos los derechos reservados.

<https://www.iso.org/obp/ui/en/#iso:std:iso-iec:20000-1:ed-3:v1:en>



Ciclo Deming PHVA Y SGS



Estructura de ISO/IEC 20000-1

1. Objeto y campo de aplicación

El alcance establece los resultados esperados del sistema de gestión. Los resultados son específicos de la industria y deben ser coherentes con el contexto de la organización (cláusula 4).

2. Referencias normativas

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

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/IEC 20000-1

4. Contexto de la organización

4.1 Comprensión de la organización y de su contexto.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas.

4.3 Determinación del alcance del sistema de gestión de servicios.

4.4 Sistema de gestión de servicios.



...

4. Contexto de la Organización



I20000IA/LA™ Versión 092020

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 a su capacidad para lograr los resultados previstos de su Sistema de Gestión de Servicios (SGS).

NOTA: el término "cuestión" en este contexto puede ser un factor que tenga un impacto positivo o negativo. Estos son factores importantes para la organización en el contexto de su capacidad para entregar servicios con la calidad acordada a sus clientes.



4.1 Comprensión de la Organización y de su Contexto

Para determinar el contexto podemos utilizar como herramientas un **Análisis FODA** (Fortalezas, Oportunidades, Debilidades y Amenazas) o un **Análisis PSET** (Político, Económico, Social, Tecnológico) entre otros.

Cuestiones externas:

- Requisitos legales reglamentarios.
- Tecnología.
- Competencia.
- Mercado.
- Cultura.
- Sociedad.
- Economía.

Cuestiones internas:

- Valores.
- Cultura.
- Conocimiento.
- Desempeño organizacional.



4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

La organización debe determinar:

- a) las partes interesadas que son pertinentes al sistema de gestión de servicios.
- b) los requisitos pertinentes de estas partes interesadas.

NOTA: los requisitos de las partes interesadas pueden incluir requisitos de servicio, rendimiento, legales y reglamentarios, y obligaciones contractuales relacionadas con el SGS y los servicios.



4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

Ejemplo de partes interesadas:

- Clientes.
- Propietarios.
- Personas.
- Proveedores.
- Banca.
- Sindicatos.
- Socios.
- Competidores.
- Otros grupos.



4.3 Determinación del Alcance del Sistema de Gestión de Servicios

La organización debe determinar los límites y la aplicabilidad del sistema de gestión de servicios para establecer su alcance.



4.4 Sistema de Gestión de Servicios

La organización debe establecer, implementar, mantener y mejorar continuamente un SGS, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de la norma.



...

5. Liderazgo



I20000IA/LA™ Versión 092020



Liderazgo

- 5. Liderazgo.
 - 5.1 Liderazgo compromiso.
 - 5.2 Política.
 - 5.3 responsabilidades autoridades en organización.

Roles,
y
la



5.1 Liderazgo y Compromiso

- a) Asegurando que se establezcan la política y los objetivos de gestión de servicios y que éstos sean compatibles con la dirección estratégica de la organización.
- b) Garantizando que se crea, implementa y mantiene un plan de gestión de servicios para respaldar la política de gestión de servicios, y el logro de los objetivos de gestión de servicios y asegurar el cumplimiento de los requisitos de servicio.
- c) Garantizando que se asignan niveles de autoridad apropiados para tomar decisiones relacionadas con el SGS y los servicios.
- d) Asegurando que se determina aquello que constituye valor para la organización y sus clientes.
- e) Asegurando que hay un control sobre las terceras partes involucradas en el ciclo de vida de los servicios.



5.1 Liderazgo y Compromiso

- f) Asegurando la integración de los requisitos del SGS en los procesos de negocio de la organización.
- g) Asegurando que los recursos necesarios para el SGS estén disponibles.
- h) Comunicando la importancia de una gestión de servicios eficaz, consiguiendo los objetivos de gestión de servicios, aportando valor y cumpliendo con los requisitos del SGS.
- i) Asegurando que el SGS logre los resultados previstos.
- j) Dirigiendo y apoyando a las personas para contribuir a la eficacia del SGS.
- k) Promoviendo la mejora continua del SGS y los servicios.
- l) Apoyando otros roles de gestión relevantes, para demostrar su liderazgo aplicado a sus áreas de responsabilidad.



5.2 Política

5.2.1 Establecimiento de la política de gestión de servicios

Se debe establecer, implementar y mantener una Política.

- a) Sea apropiada al propósito de la organización.
- b) Proporcione un marco de referencia para el establecimiento de los objetivos de gestión de servicios.
- c) Incluya un compromiso de cumplir los requisitos aplicables.
- d) Incluya un compromiso de mejora continua del sistema de gestión de servicios y los servicios.



5.2 Política

5.2.2 Comunicación de la política de gestión de servicios

La política debe:

- a) Estar disponible y mantenerse como información documentada.
- b) Comunicarse, entenderse y aplicarse dentro de la organización.
- c) Estar disponible para las partes interesadas pertinentes, según corresponda.



5.2 Política

5.3 Roles, responsabilidades y autoridades de la organización

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

La alta dirección debe asignar responsabilidad y autoridad para:

- a) Asegurar que el SGS es conforme con los requisitos de este documento.
- b) Informar a la alta dirección sobre el desempeño del SGS y los servicios.



...

6. Planificación



I20000IA/LA™ Versión 092020



Planificación

- 6. Planificación.
 - 6.1 Acciones para abordar riesgos y oportunidades.
 - 6.2 Objetivos de gestión de servicios y planificación para su consecución.
 - 6.3 Planificar el sistema de gestión de servicios.



6.1 Acciones para Abordar Riesgos y Oportunidades

6.1.1 Al planificar el SGS, 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 SGS pueda lograr sus resultados previstos.
- b)** Prevenir o reducir efectos no deseados.
- c)** Lograr la mejora continua del SGS y de los servicios.

6.1.2 La organización debe determinar y documentar:

- a)** Los riesgos relacionados con:
 1. La organización.
 2. El no cumplimiento de los requisitos de servicio.
 3. La involucración de otras partes en el ciclo de vida de los servicios.
- b)** El impacto de los riesgos en los clientes y las oportunidades para el SGS y los servicios.
- c)** Los criterios de aceptación de riesgos.
- d)** La aproximación a seguir para la gestión de riesgos.



6.1 Acciones para Abordar Riesgos y Oportunidades

6.1.3 La organización debe planificar:

- a) Las acciones para tratar estos riesgos y oportunidades y sus prioridades.
- b) La manera de:
 - 1) Integrar e implementar las acciones en los procesos del SGS.
 - 2) Evaluar la eficacia de estas acciones.
- **NOTA 1:** Las opciones para tratar los riesgos y las oportunidades pueden incluir: evitar el riesgo, asumir o aumentar el riesgo para continuar con una oportunidad, eliminar el origen del riesgo, modificar la probabilidad o relevancia del riesgo, mitigar el riesgo mediante acciones acordadas, compartir el riesgo con otra parte o aceptar el riesgo con una decisión fundamentada.
- **NOTA 2:** La Norma ISO 31000 proporciona principios y directrices genéricas sobre gestión de riesgos.



6.2 Objetivos de Gestión de Servicios y Planificación para su Consecución

6.2.2 Planificar la consecución de los objetivos

- 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 Planificar el Sistema de Gestión de Servicios

La organización debe crear, implementar y mantener un plan de gestión de servicios. El plan debe tener en cuenta la política de gestión de servicios, los objetivos, riesgos y oportunidades de gestión de servicios, los requisitos de servicio y los requisitos especificados en este documento.



6.3 Planificar el Sistema de Gestión de Servicios

El plan de gestión de servicios debe incluir o hacer referencia a:

- a) La lista de servicios.
- b) Las limitaciones conocidas que pueden afectar al SGS y los servicios.
- c) Las obligaciones tales como políticas relevantes, normas o estándares, requisitos legales, reglamentarios y contractuales, y cómo estas obligaciones se aplican al SGS y los servicios.
- d) Autoridades y responsabilidades para el SGS y los servicios.
- e) Recursos humanos, técnicos, de información y financieros necesarios para operar el SGS y los servicios.



6.3 Planificar el Sistema de Gestión de Servicios

El plan de gestión de servicios debe incluir o hacer referencia a:

- f) El enfoque que debe tomarse para trabajar con otras partes involucradas en el ciclo de vida de los servicios.
- g) La tecnología utilizada para apoyar el SGS.
- h) Cómo se medirá, auditará, informará y mejorará la eficacia del SGS y los servicios.

Otras actividades de planificación deben mantener la alineación con el plan de gestión de servicios.



...

7. Apoyo (Soporte)



I20000IA/LA™ Versión 092020



Apoyo

- 7. Apoyo.
 - 7.1 Recursos.
 - 7.2 Competencia.
 - 7.3 Concienciación.
 - 7.4 Comunicación.
 - 7.5 Información documentada.
 - 7.6 Conocimiento.



7.1 Recursos

La organización debe determinar y proporcionar los recursos humanos, técnicos, de información y financieros necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGS y la operación de los servicios para cumplir los requisitos de servicio y alcanzar los objetivos de gestión de servicios.



7.2 Competencia

La organización debe:

- a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecte al desempeño y eficacia del SGS y de los servicios.
- b) Asegurar que estas personas sean competentes, basándose en la educación, formación o experiencia apropiadas.
- c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.
- d) Conservar la información documentada que sea 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 el trabajo bajo el control de la organización deben ser conscientes de:

- La política de gestión de servicios.
- Los objetivos de gestión de servicios.
- Los servicios relevantes para su trabajo.
- Su contribución a la eficacia del SGS, incluidos los beneficios de una mejora del desempeño.
- Las implicaciones del incumplimiento de los requisitos del SGS.



7.4 Comunicación

Incluye la determinación de las comunicaciones internas y externas relevantes al SGS y los servicios.

- Qué comunicar.
- Cuándo comunicar.
- A quién comunicar.
- Cómo comunicar.
- Quién comunica.



7.5 Información Documentada

7.5.1 Generalidades

El SGS 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 SGS.

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

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



7.5 Información Documentada

7.5.2 Creación y actualización de la información documentada

Asegurarse de que sea apropiado:

- La identificación y descripción (por ejemplo, título, fecha, autor o número de referencia).
- El formato (por ejemplo, idioma, versión del software, gráficos) y los medios de soporte (por ejemplo, papel, electrónico).
- Revisión y aprobación de idoneidad y adecuación.



7.5 Información Documentada

7.5.3 Control de la información documentada

7.5.3.1 Control para asegurar

- Disponibilidad e idoneidad para su uso, donde y cuando se necesite.
- Protección adecuada (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado o pérdida de integridad).



7.5 Información Documentada

7.5.3.2 Actividades de control

- a) Distribución, acceso, recuperación y uso.
 - b) Almacenamiento y preservación, incluida la preservación de la legibilidad.
 - c) Control de cambios.
 - d) Conservación y disposición.
-
- Información documentada de origen externo se debe identificar, según sea apropiado, y controlar.
 - La información documentada conservada como evidencia de la conformidad debe protegerse contra modificaciones no intencionadas.



7.5 Información Documentada

7.5.4 Información documentada del sistema de gestión de servicios

La información documentada del SGS debe incluir:

- a) Alcance del SGS.
- b) Política y objetivos de gestión de servicios.
- c) Plan de gestión de servicios.
- d) Política de gestión de cambios, política de seguridad de la información y el plan o planes de continuidad de los servicios.
- e) Procesos del SGS de la organización.
- f) Requisitos de servicio.



7.5 Información Documentada

- g) Catálogo o catálogos de servicios.
- h) Acuerdo o acuerdos de nivel de servicio (SLA).
- i) Contratos con proveedores externos.
- j) Acuerdos con proveedores internos o clientes que actúen como proveedores.
- k) Procedimientos requeridos por este documento.
- l) Registros requeridos para demostrar evidencia de conformidad con los requisitos de este documento del SGS de la organización.



7.6 Conocimiento

La organización debe determinar y mantener el conocimiento necesario para apoyar el funcionamiento del SGS y los servicios.

El conocimiento debe ser relevante, utilizable y estar disponible para las personas adecuadas.



• • •

8. Operación



I20000IA/LA™ Versión 092020



Operación

- 8. Operación.
 - 8.1 Planificación y control operacional.
 - 8.2 Portafolio de servicios.
 - 8.3 Relación y acuerdo.
 - 8.4 Oferta y demanda.
 - 8.5 Producción y provisión del servicio.
 - 8.6 Resolución y ejecución.
 - 8.7 Aseguramiento de servicios.



8.1 Planificación y Control Operacional

Planificar, implementar y controlar los procesos necesarios para cumplir los requisitos.

- a) Estableciendo los criterios de desempeño para los procesos en función de los requisitos.
- b) Implementando el control de los procesos de acuerdo con los criterios de desempeño establecidos.
- c) Manteniendo la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados al SGS y revisar las consecuencias de los cambios imprevistos, llevando a cabo acciones para mitigar los efectos adversos según sea necesario.



8.2 Portafolio de Servicios

8.2.1 Prestación de servicios

La organización debe operar el SGS asegurando la coordinación de las actividades y los recursos. La organización debe llevar a cabo las actividades requeridas para prestar los servicios.

NOTA: se utiliza un portafolio de servicios para gestionar el ciclo de vida completo de todos los servicios, incluidos los servicios propuestos, los que están en desarrollo, los servicios activos definidos en el catálogo o catálogos de servicios y los servicios que deben ser retirados. La gestión del portafolio de servicios garantiza que el proveedor de servicios tiene la combinación adecuada de servicios. Las actividades del portafolio de servicios en este documento incluyen la planificación de los servicios, el control de las partes involucradas en el ciclo de vida de los servicios, la gestión del catálogo de servicios, la gestión de activos y la gestión de la configuración.



8.2 Portafolio de Servicios

8.2.2 Planificación de servicios

- Determinar y documentar los requisitos de servicio para servicios existentes, nuevos servicios y para cambios en los servicios.
- Determinar la criticidad de los servicios en función de las necesidades de la organización, los clientes, los usuarios y otras partes interesadas. La organización debe determinar y gestionar las dependencias y la duplicidad entre servicios.
- Proponer cambios, donde sea necesario, para alinear los servicios con la política de gestión de servicios, los objetivos de gestión de servicios y los requisitos de los servicios, teniendo en cuenta las limitaciones y los riesgos conocidos.
- Priorizar las peticiones de cambio y las propuestas de servicios nuevos o modificados para alinearse con las necesidades de negocio y los objetivos de gestión de servicios teniendo en cuenta los recursos disponibles.



8.2 Portafolio de Servicios

8.2.3 Control de partes involucradas en el ciclo de vida de los servicios

8.2.3.1 La organización debe mantener la [completa/total] responsabilidad sobre los requisitos especificados en este documento y sobre la prestación de los servicios, independientemente de qué parte esté involucrada en la realización de actividades para apoyar el ciclo de vida de los servicios.

Determinar y aplicar criterios para la evaluación y selección de terceros involucrados en el ciclo de vida de los servicios. Terceros pueden ser un proveedor externo, un proveedor interno o un cliente que actúa como proveedor.



8.2 Portafolio de Servicios

Los terceros no deben proporcionar u operar todos los servicios, componentes de servicios o procesos dentro del alcance del SGS.
La organización debe determinar y documentar:

- a) Los servicios proporcionados u operados por terceros.
- b) Los componentes de servicios que son provistos u operados por terceros.
- c) Los procesos, o partes de procesos, en el SGS de la organización que son operados por terceros.

Integrar los servicios, los componentes de servicios y los procesos en el SGS provistos u operados por la organización o terceros para cumplir con los requisitos de los servicios. La organización debe coordinar las actividades con terceros involucradas en el ciclo de vida de los servicios, incluida la planificación, el diseño, la transición, la prestación y la mejora de los servicios.



8.2 Portafolio de Servicios

8.2.3.2 La organización debe definir y aplicar a los terceros controles relevantes de entre los siguientes:

- a) Medición y evaluación del rendimiento de los procesos.
- b) Medición y evaluación de la eficacia de los servicios y componentes de servicios para cumplir los requisitos de los servicios.



8.2 Portafolio de Servicios

8.2.4 Gestión del catálogo de servicios

Crear y mantener uno o más catálogos de servicios. El catálogo o catálogos de servicios deben incluir información para la organización, los clientes, los usuarios y otras partes interesadas para describir los servicios, sus resultados esperados y las dependencias entre los servicios.

Dar acceso a las partes apropiadas del catálogo o catálogos de servicios a sus clientes, usuarios y otras partes interesadas.

8.2.5 Gestión de activos

Asegurar que los activos utilizados para prestar los servicios están gestionados para cumplir con los requisitos de los servicios y las obligaciones definidas en el apartado 6.3 c).



8.2 Portafolio de Servicios

8.2.6 Gestión de la configuración

Se deben definir los tipos de elementos de configuración (CI). Los servicios se deben clasificar como elementos de configuración (CI).

La información de configuración debe registrarse a un nivel de detalle acorde con la criticidad y tipo de servicios. Debe controlarse el acceso a la información de configuración. La información de configuración registrada para cada CI debe incluir:

- a) Identificación única.
- b) Tipo de CI.
- c) Descripción del CI.
- d) Relación con otros CI.
- e) Estado.



8.2 Portafolio de Servicios

Los CI deben estar controlados. Los cambios a los CI deben ser trazables y auditables para mantener la integridad de la información de configuración. La información de configuración debe actualizarse después de implementar cambios en los CI.

Verificar la exactitud de la información de configuración a intervalos planificados. Donde se encuentren deficiencias, la organización debe llevar a cabo las acciones necesarias.

La información de configuración debe estar disponible para otras actividades de gestión de servicios, según corresponda.



8.3 Relación y Acuerdo

8.3.1 Generalidades

La organización puede usar proveedores para:

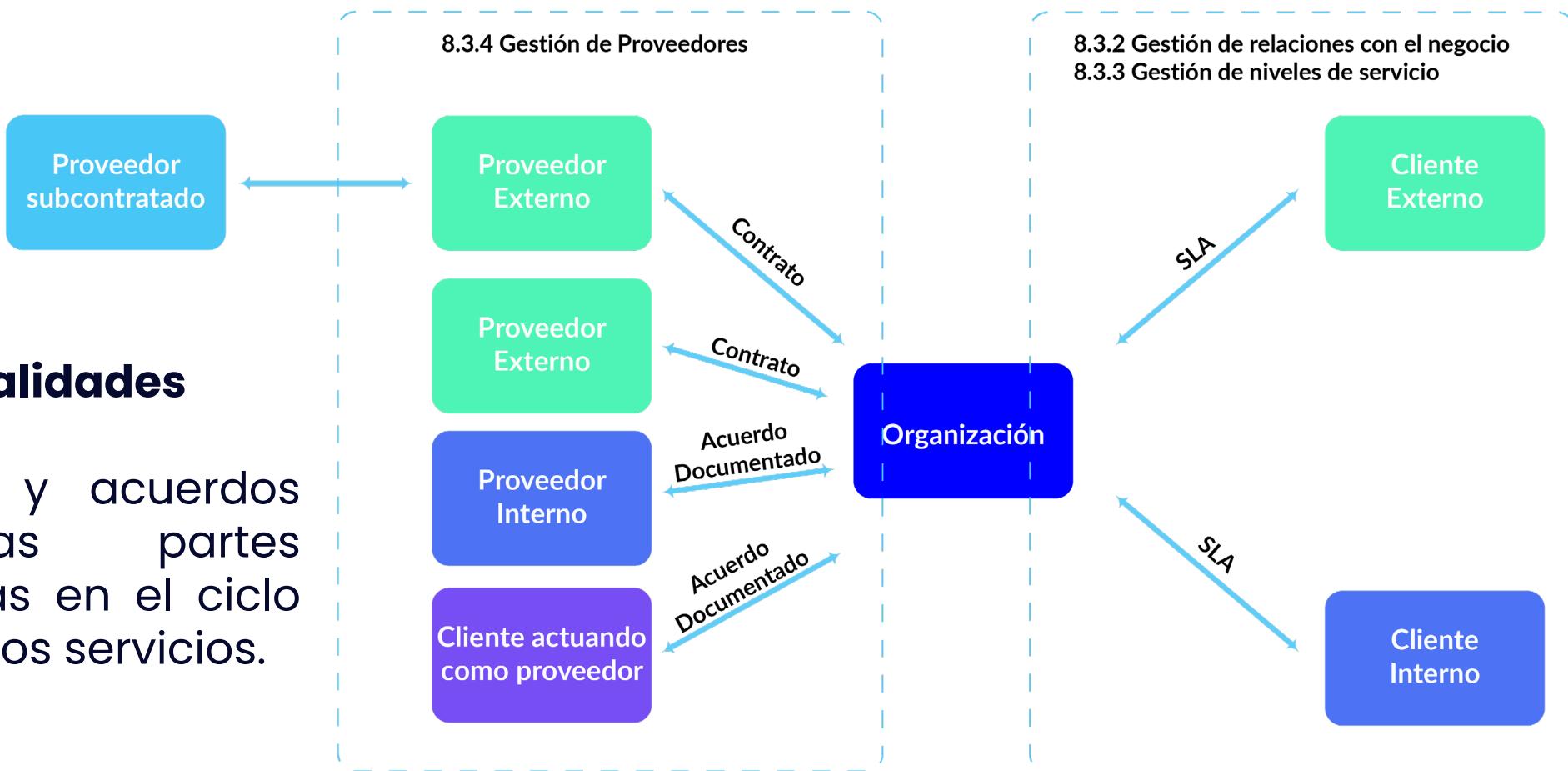
- a) Prestar u operar servicios.
- b) Prestar u operar componentes de servicios.
- c) Operar procesos, o partes de procesos, que están en el SGS de la organización.



8.3 Relación y Acuerdo

8.3.1 Generalidades

Relaciones y acuerdos entre las partes involucradas en el ciclo de vida de los servicios.



8.3 Relación y Acuerdo

8.3.2 Gestión de relaciones con el negocio

Se deben identificar y documentar los clientes, usuarios y otras partes interesadas de los servicios. La organización debe tener una o más personas designadas como responsables de la gestión de las relaciones con los clientes y del mantenimiento de su satisfacción.

La organización debe establecer acuerdos de comunicación con sus clientes y otras partes interesadas.

La comunicación debe promover el entendimiento del entorno empresarial cambiante en el que operan los servicios y debe capacitar a la organización para dar respuesta a los requisitos de servicio nuevos o modificados.



8.3 Relación y Acuerdo

La organización debe revisar las tendencias del rendimiento y los resultados de los servicios a intervalos planificados.

La organización debe medir, a intervalos planificados, la satisfacción con los servicios, apoyándose en una muestra representativa de clientes. Los resultados deben ser analizados, revisados para identificar oportunidades de mejora, y ser comunicados.

Se deben registrar, gestionar hasta su cierre y comunicar las reclamaciones de los servicios. Cuando una reclamación de servicio no pueda resolverse mediante los canales normales, debe proporcionarse un método de escalado.



8.3 Relación y Acuerdo

8.3.3 Gestión de niveles de servicio

La organización y los clientes deben acordar los servicios a ser prestados.

Para cada servicio prestado, la organización debe establecer uno o más SLA basados en los requisitos de servicio documentados. Los SLA deben incluir los objetivos de nivel de servicio, los límites de volumen de trabajo y las excepciones.

La organización debe monitorizar, revisar e informar a intervalos planificados:

- a) El desempeño frente a los objetivos de nivel de servicio.
- b) Los cambios actuales y periódicos del volumen de trabajo comparados con los límites descritos en los SLA.

Cuando no se cumplan los objetivos de nivel de servicio, la organización debe identificar oportunidades de mejora.



8.3 Relación y Acuerdo

8.3.4 Gestión de proveedores

8.3.4.1 Gestión de proveedores externos

La organización debe contar con una o más personas designadas como responsables de gestionar las relaciones, los contratos y el desempeño de los proveedores externos.

La organización debe acordar un contrato documentado para cada proveedor externo. El contrato debe incluir o contener una referencia a:

- a) El alcance de los servicios, los componentes de servicios, los procesos o partes de los procesos a ser provistos u operados por el proveedor externo.
- b) Los requisitos que debe cumplir el proveedor externo.
- c) Los objetivos de nivel de servicio u otras obligaciones contractuales.
- d) Las autoridades y responsabilidades de la organización y el proveedor externo.



8.3 Relación y Acuerdo

La organización debe evaluar la alineación de los objetivos de nivel de servicio u otras obligaciones contractuales con el proveedor externo frente a los SLA con los clientes, y tratar los riesgos identificados.

La organización debe definir y gestionar las interfaces con el proveedor externo.

La organización debe monitorizar, a intervalos planificados, el desempeño del proveedor externo.

Cuando no se cumplan los objetivos de nivel de servicio u otras obligaciones contractuales, la organización debe garantizar que se identifiquen oportunidades de mejora.



8.3 Relación y Acuerdo

La organización debe revisar el contrato frente a los requisitos de servicio vigentes a intervalos planificados.

Los cambios identificados en el contrato deben evaluarse por el impacto de dichos cambios en el SGS y en los servicios antes de su aprobación.

Los desacuerdos entre la organización y el proveedor externo deben registrarse y gestionarse hasta su cierre.



8.3 Relación y Acuerdo

8.3.4.2 Gestión de proveedores internos y clientes actuando como proveedores

Para cada proveedor interno o cliente actuando como proveedor, la organización debe desarrollar, acordar y mantener un acuerdo documentado para definir los objetivos de nivel de servicio, otros compromisos, actividades e interfaces entre las partes.

La organización debe monitorizar el desempeño del proveedor interno o del cliente que actúa como proveedor a intervalos planificados. Cuando no se cumplan los objetivos de nivel de servicio u otros compromisos acordados, la organización debe garantizar que se identifiquen oportunidades de mejora.



8.4 Oferta y Demanda

8.4.1 Presupuesto y contabilidad de servicios

La organización debe presupuestar y contabilizar servicios o grupos de servicios de acuerdo con sus políticas y procesos de gestión financiera.

Los costes deben presupuestarse para permitir el control financiero efectivo y la toma de decisiones sobre los servicios.

La organización debe monitorizar e informar a intervalos planificados sobre los costes reales con respecto al presupuesto, revisar las previsiones financieras y gestionar los costes.



8.4 Oferta y Demanda

8.4.2 Gestión de la demanda

La organización debe, a intervalos planificados:

- a) Determinar la demanda actual y estimar la demanda futura de los servicios.
- b) Monitorizar e informar sobre la demanda y el consumo de los servicios.



8.4 Oferta y Demanda

8.4.3 Gestión de la capacidad

Se deben determinar, documentar y mantener los requisitos de capacidad para los recursos humanos, técnicos, de información y financieros teniendo en cuenta los requisitos de servicio y rendimiento.

La organización debe planificar la capacidad para incluir:

- a) La capacidad actual y prevista en función de la demanda de los servicios.
- b) El impacto esperado en la capacidad de los objetivos de nivel de servicio acordados, en los requisitos de disponibilidad y continuidad de servicios.
- c) Escalas de tiempo y umbrales para cambios en la gestión de la capacidad.

Proporcionar la capacidad suficiente para cumplir con los requisitos acordados de capacidad y rendimiento. La organización debe monitorizar el uso de la capacidad, analizar los datos de capacidad y rendimiento e identificar oportunidades para mejorar dicho rendimiento.



8.5 Diseño, Construcción y Transición de Servicios

8.5.1 Gestión de cambios

8.5.1.1 Política de gestión de cambios

Se debe establecer y documentar una política de gestión de cambios para definir:

- a) Los componentes de servicios y otros elementos que están bajo el control de la gestión de cambios.
- b) Las categorías de cambio, incluido el cambio de emergencia, y cómo se deben gestionar.
- c) Los criterios para determinar los cambios con el potencial de tener un gran impacto en los clientes o en los servicios.



8.5 Diseño, Construcción y Transición de Servicios

8.5.1.2 Inicio de la gestión de cambios

Deben registrarse y clasificarse las peticiones de cambio, incluidas las propuestas para incorporar, retirar o transferir servicios.

- a) Los servicios nuevos con el potencial de tener un gran impacto en los clientes o en otros servicios según lo establecido en la política de gestión de cambios.
- b) Los cambios en los servicios con el potencial de tener un gran impacto en los clientes o en otros servicios según lo establecido en la política de gestión de cambios.
- c) Las categorías de cambio que deben ser gestionadas por el diseño y transición de servicios de acuerdo con la política de gestión de cambios.



8.5 Diseño, Construcción y Transición de Servicios

- d) La retirada de un servicio.
- e) La transferencia de un servicio existente desde la organización a un cliente o tercero.
- f) La transferencia de un servicio existente desde un cliente o tercero a la organización.

La evaluación, aprobación, programación y revisión de los servicios nuevos o modificados en el alcance del apartado 8.5.2 deben gestionarse mediante las actividades de gestión de cambios del apartado 8.5.1.3.

Las peticiones de cambio que no se gestionan mediante del apartado 8.5.2 deben gestionarse mediante las actividades de gestión de cambios del apartado 8.5.1.3.



8.5 Diseño, Construcción y Transición de Servicios

8.5.1.3 Actividades de gestión de cambios

La organización y las partes interesadas deben tomar decisiones sobre la aprobación y la prioridad de las peticiones de cambio. La toma de decisiones debe tener en cuenta los riesgos, los beneficios de negocio, la viabilidad y el impacto financiero.



8.5 Diseño, Construcción y Transición de Servicios

La toma de decisiones debe considerar también los impactos potenciales del cambio en:

- a) Los servicios existentes.
- b) Los clientes, usuarios y otras partes interesadas.
- c) Las políticas y planes requeridos por este documento.
- d) La capacidad, disponibilidad de los servicios, continuidad de los servicios y seguridad de la información.
- e) Otras peticiones de cambio, entregas y planes de despliegue.



8.5 Diseño, Construcción y Transición de Servicios

Los cambios aprobados deben ser preparados, verificados y, cuando sea posible, probados. Se debe comunicar a las partes interesadas las fechas propuestas de implementación y otros detalles de implementación de los cambios aprobados.

Se deben planificar, y cuando sea posible probar, las actividades necesarias para revertir o remediar un cambio fallido. Los cambios fallidos deben analizarse y acordar las acciones a llevar a cabo.

La organización debe revisar los cambios para comprobar su eficacia y llevar a cabo las acciones acordadas con las partes interesadas.

Los registros de peticiones de cambio deben analizarse a intervalos planificados, para detectar tendencias. Los resultados y conclusiones extraídos del análisis deben registrarse y revisarse para identificar oportunidades de mejora.



8.5 Diseño, Construcción y Transición de Servicios

8.5.2 Diseño y transición de servicios

8.5.2.1 Planificación de servicios nuevos o modificados

La planificación debe usar los requisitos de servicio para los servicios nuevos o modificados determinados en el apartado 8.2.2 y debe incluir o contener una referencia a:

- a) Las autoridades y responsabilidades sobre las actividades de diseño, construcción y transición.
- b) Las actividades a realizar por la organización u otras partes con sus plazos.
- c) Los recursos humanos, técnicos, de información y financieros.
- d) Las dependencias de otros servicios.



8.5 Diseño, Construcción y Transición de Servicios

- e) Las pruebas necesarias para los servicios nuevos o modificados.
- f) Los criterios de aceptación de servicios.
- g) Los resultados esperados de la prestación de los servicios nuevos o modificados, expresados en términos medibles.
- h) El impacto en el SGS, en otros servicios, en cambios planificados, en clientes, en usuarios y en otras partes interesadas.



8.5 Diseño, Construcción y Transición de Servicios

Para los servicios que deben ser retirados, la planificación debe incluir además la fecha o fechas para la retirada de los servicios y las actividades de archivo, eliminación o transferencia de datos, de información documentada y de componentes de servicios.

Para los servicios que deben ser transferidos, la planificación debe incluir además la fecha o fechas para la transferencia de los servicios y las actividades para la transferencia de datos, de información documentada, de conocimiento y de componentes de servicios.

Los CI afectados por los servicios nuevos o modificados deben gestionarse mediante la gestión de la configuración.



8.5 Diseño, Construcción y Transición de Servicios

8.5.2.2 Diseño

Los servicios nuevos o modificados deben diseñarse y documentarse para cumplir con los requisitos de servicio determinados en el apartado 8.2.2. El diseño debe incluir los elementos relevantes de entre los siguientes:

- a) Las autoridades y responsabilidades de las partes involucradas en la prestación de los servicios nuevos o modificados.
- b) Los requisitos para cambios en los recursos humanos, técnicos, de información y financieros.
- c) Los requisitos para una formación, capacitación y experiencia adecuados.
- d) Los SLAs nuevos o modificados, contratos y otros acuerdos documentados en los que se apoyan los servicios.



8.5 Diseño, Construcción y Transición de Servicios

- e) Cambios que afectan a SGS, incluidas adiciones o cambios en políticas, planes, procesos, procedimientos, medidas y conocimientos.
- f) El impacto en otros servicios.
- g) Las actualizaciones del catálogo o catálogos de servicios.



8.5 Diseño, Construcción y Transición de Servicios

8.5.2.3 Construcción y transición

Los servicios nuevos o modificados se deben construir y probar para verificar que cumplen con los requisitos de servicio, que se ajustan al diseño documentado y que cumplen con los criterios acordados de aceptación de servicios. Si no se cumplen los criterios de aceptación de servicios, la organización y las partes interesadas deben decidir sobre las acciones necesarias y el despliegue de los servicios.

Se debe utilizar la gestión de entregas y despliegues para desplegar los servicios nuevos o modificados aprobados en el entorno de producción.

Después de la finalización de las actividades de transición, la organización debe informar a las partes interesadas sobre los resultados obtenidos frente a los esperados.



8.5 Diseño, Construcción y Transición de Servicios

8.5.3 Gestión de entregas y despliegues

Definir los tipos de entregas, incluida la entrega de emergencia, su frecuencia y la forma en que se gestionan.

Planificar el despliegue de servicios nuevos o modificados y componentes de servicios en el entorno de producción. La planificación debe estar coordinada con la gestión de cambios e incluir referencias a las peticiones de cambio relacionadas, errores conocidos o problemas que se resuelven mediante de la entrega. La planificación debe incluir las fechas para el despliegue de cada entrega, los entregables y los métodos de despliegue.

La entrega debe ser verificada frente a los criterios de aceptación documentados y aprobada antes del despliegue. Si los criterios de aceptación no se cumplen, la organización y las partes interesadas deben decidir sobre las acciones necesarias y el despliegue.



8.5 Diseño, Construcción y Transición de Servicios

Se debe capturar una línea base de configuración de los CI afectados antes del despliegue de una entrega en el entorno de producción.

La entrega se debe desplegar en el entorno de producción de manera que se mantenga la integridad de los servicios y los componentes de servicios.

El éxito o el fallo de las entregas se debe monitorizar y analizar. Las medidas deben incluir las incidencias relacionadas con una entrega en el período posterior al despliegue de dicha entrega. Los resultados y conclusiones extraídos de los análisis se deben registrar y revisar para identificar oportunidades de mejora.

La información sobre el éxito o el fallo de las entregas y las fechas de futuras entregas deben estar disponibles para otras actividades de gestión de servicios, según corresponda.



8.6 Resolución y Ejecución

8.6.1 Gestión de incidencias

Las incidencias deben ser:

- a) Registradas y clasificadas.
- b) Priorizadas teniendo en cuenta el impacto y la urgencia.
- c) Escaladas si es necesario.
- d) Resueltas.
- e) Cerradas.

Los registros de incidencias se deben actualizar con las acciones llevadas a cabo durante las mismas.

Determinar los criterios para identificar una incidencia grave. Las incidencias graves deben ser clasificadas y gestionadas de acuerdo a un procedimiento documentado.



8.6 Resolución y Ejecución

8.6.2 Gestión de peticiones de servicio

Las peticiones de servicio deben ser:

- a) Registradas y clasificadas.
- b) Priorizadas.
- c) Satisfechas.
- d) Cerradas.

Los registros de las peticiones de servicio se deben actualizar con las acciones llevadas a cabo durante las mismas.

Las instrucciones para la ejecución de las peticiones de servicio deben estar a disposición de las personas involucradas en la ejecución de peticiones de servicio.



8.6 Resolución y Ejecución

8.6.3 Gestión de problemas

Analizar datos y tendencias sobre incidencias para identificar problemas. La organización debe llevar a cabo un análisis de la causa raíz y determinar las posibles acciones para prevenir la ocurrencia o repetición de las incidencias.

Los problemas deben ser:

- a) Registrados y clasificados.
- b) Priorizados.
- c) Escalados, si es necesario.
- d) Resueltos, si es posible.
- e) Cerrados.



8.6 Resolución y Ejecución

Los registros de problemas se deben actualizar con las acciones llevadas a cabo. Los cambios necesarios para la resolución de problemas se deben gestionar de acuerdo con la política de gestión de cambios.

Cuando la causa raíz ha sido identificada, pero el problema no ha sido resuelto de manera definitiva, la organización debe determinar acciones para reducir o eliminar el impacto del problema en los servicios. Los errores conocidos deben ser registrados. La información actualizada sobre los errores conocidos y las resoluciones de problemas deben ser puestos a disposición de otras actividades de gestión de servicios según corresponda.

La eficacia de la resolución de problemas debe ser monitorizada, revisada y reportada a intervalos planificados.



8.7 Aseguramiento de Servicios

8.7.1 Gestión de la disponibilidad de servicios

Se deben evaluar y documentar los riesgos sobre la disponibilidad de los servicios a intervalos planificados.

La organización debe determinar los requisitos y objetivos de disponibilidad de los servicios.

Los requisitos acordados deben tener en cuenta los requisitos de negocio relevantes, los requisitos de servicio, los SLAs y los riesgos.

Se deben documentar y mantener los requisitos y los objetivos de disponibilidad de los servicios.

Se debe monitorizar la disponibilidad de los servicios, registrar los resultados y compararlos con los objetivos. Se debe investigar la indisponibilidad no planificada y llevar a cabo las acciones necesarias.



8.7 Aseguramiento de Servicios

8.7.2 Gestión de la continuidad de los servicios

Se deben evaluar y documentar los riesgos sobre la continuidad de los servicios a intervalos planificados. La organización debe determinar los requisitos de continuidad de los servicios. Los requisitos acordados deben tener en cuenta los requisitos relevantes de negocio, los requisitos de los servicios, los SLAs y los riesgos.



8.7 Aseguramiento de Servicios

La organización debe crear, implementar y mantener uno o más planes de continuidad de los servicios.

El plan o planes de continuidad de los servicios deben incluir o hacer referencia a:

- a) Los criterios y las responsabilidades para invocar la continuidad de los servicios.
- b) Los procedimientos que se pondrán en marcha en caso de una pérdida grave de servicio.
- c) Los objetivos de disponibilidad de servicio cuando se invoca el plan de continuidad de los servicios.
- d) Los requisitos de recuperación de los servicios.
- e) Los procedimientos para volver a las condiciones normales de trabajo.



8.7 Aseguramiento de Servicios

Cuando no se pueda acceder a la ubicación normal de prestación de los servicios se debe tener acceso al plan o planes de continuidad de los servicios y a la lista de contactos.

Probar el plan o planes de continuidad de los servicios frente a los requisitos de continuidad de servicio a intervalos planificados. El plan o planes de continuidad de los servicios se deben volver a probar tras cambios significativos en el entorno de servicio. Los resultados de las pruebas deben ser registrados. Deben realizarse revisiones después de cada prueba y después de que el plan o planes de continuidad de servicio hayan sido invocados. Cuando se encuentren deficiencias, la organización debe llevar a cabo las acciones necesarias.

Informar sobre la causa, el impacto y la recuperación una vez que se haya invocado el plan o planes de continuidad de los servicios.



8.7 Aseguramiento de Servicios

8.7.3 Gestión de la seguridad de la información

8.7.3.1 Política de seguridad de la información

Los miembros de la dirección con el nivel adecuado de autoridad deben aprobar una política de seguridad de la información relevante para la organización. La política de seguridad de la información debe estar documentada y tener en consideración los requisitos de servicio y las obligaciones del apartado 6.3 c).

La política de seguridad de la información debe estar disponible según corresponda. La organización debe comunicar la importancia de cumplir con la política de seguridad de la información y su aplicabilidad al SGS y los servicios a las personas apropiadas dentro de:

- a) La organización.
- b) Los clientes y los usuarios.
- c) Los proveedores externos e internos y otras partes interesadas.



8.7 Aseguramiento de Servicios

8.7.3.2 Controles de seguridad de la información

Evaluar y documentar, a intervalos planificados, los riesgos de seguridad de la información para el SGS y los servicios. Se deben determinar, implementar y operar los controles de seguridad de la información para dar soporte la política de seguridad de la información y tratar los riesgos de seguridad de la información identificados. Deben documentarse las decisiones sobre los controles de seguridad de la información.

Acordar e implementar controles de seguridad de la información para abordar los riesgos de seguridad de la información relacionados con organizaciones externas.

Monitorizar y revisar la eficacia de los controles de seguridad de la información y llevar a cabo las acciones necesarias.



8.7 Aseguramiento de Servicios

8.7.3.3 Incidencias de seguridad de la información

Las incidencias de seguridad de la información deben ser:

- a) Registradas y clasificadas.
- b) Priorizadas tomando en consideración los riesgos de seguridad de la información.
- c) Escaladas si es necesario.
- d) Resueltas.
- e) Cerradas.

Analizar las incidencias de seguridad de la información por tipo, volumen e impacto en el SGS, los servicios y las partes interesadas. Las incidencias de seguridad de la información deben ser comunicadas y revisadas para identificar oportunidades de mejora.



...

9. Evaluación del Desempeño



I20000IA/LA™ Versión 092020



Evaluación del Desempeño

- 9. Evaluación del desempeño.
 - 9.1 Monitorización, medición, análisis y evaluación.
 - 9.2 Auditoría interna.
 - 9.3 Revisión por la dirección.
 - 9.4 Informes de Servicio.



9.1 Monitorización, Medición, Análisis y Evaluación

La organización debe determinar:

- a) Qué es necesario monitorizar y qué es necesario medir para el SGS y los servicios.
- b) Los métodos de monitorización, medición, análisis y evaluación, según sea aplicable, para garantizar resultados válidos.
- c) Cuándo se deben llevar a cabo la monitorización y la medición.
- d) Cuándo se deben analizar y evaluar los resultados de la monitorización y de la medición.

Conservar la información documentada adecuada como evidencia de los resultados. La organización debe evaluar el desempeño del SGS frente a los objetivos de gestión de servicios y evaluar la eficacia del SGS. La organización debe evaluar la eficacia de los servicios frente a los requisitos de servicio.



9.2 Auditoría Interna

9.2.1 La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información acerca de si el sistema de gestión de la calidad:

- a) Cumple con:
 1. Los requisitos propios de la organización para su sistema de gestión de servicios.
 2. Los requisitos de esta Norma.
- b) Se implementa y mantiene eficazmente.



9.2 Auditoría Interna

9.2.2 La organización debe:

- a) Planificar, establecer, implementar y mantener uno o varios programas de auditoría.
- b) Definir los criterios y el alcance para cada auditoría.
- c) Seleccionar auditores y realizar auditorías para garantizar la objetividad y la imparcialidad del proceso de auditoría.
- d) Asegurar que se informa a la dirección de los resultados de las auditorías.
- e) Conservar información documentada como evidencia de la implementación del programa o programas de auditoría y de los resultados de auditoría.



9.3 Revisión por la Dirección

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

Entradas de la revisión por la dirección



Revisión por
la dirección



Salidas de la revisión por la dirección



9.3 Revisión por la Dirección

La revisión por la dirección debe incluir consideraciones sobre:

- a) El estado de las acciones derivadas de las revisiones por la dirección previas.
- b) Los cambios en las cuestiones externas e internas que afecten al SGS.
- c) Información sobre el desempeño y la eficacia del SGS, incluidas las tendencias relativas a:
 - 1. Las no conformidades y acciones correctivas.
 - 2. Los resultados de la monitorización y la medición.
 - 3. Los resultados de las auditorías.



9.3 Revisión por la Dirección

- d) Las oportunidades de mejora continua.
- e) La retroalimentación de los clientes y otras partes interesadas.
- f) La idoneidad y el compromiso con la política de gestión de servicios y otras políticas requeridas por este documento.
- g) La consecución de los objetivos de gestión de servicio.
- h) El rendimiento de los servicios.
- i) El desempeño de otras partes involucradas en la prestación de los servicios.
- j) Los niveles actuales y previstos de recursos humanos, técnicos, de información y financieros, y las capacidades de los recursos humanos y técnicos.
- k) Los resultados del análisis de riesgos y la eficacia de las medidas adoptadas para gestionar los riesgos y las oportunidades.
- l) Los cambios que pueden afectar el SGS y los servicios.



9.3 Revisión por la Dirección

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambio en el SGS y los servicios.

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



9.4 Informes de Servicio

Determinar los requisitos de los informes y su propósito.

Generar informes sobre el rendimiento y la eficacia del SGS y los servicios utilizando la información de las actividades del SGS y de la prestación de los servicios. Los informes de servicios deben incluir tendencias.

Decidir y llevar a cabo acciones fundamentadas en las conclusiones de los informes de servicio. Las acciones acordadas se deben comunicar a las partes interesadas.



• • •

10. Mejora



I20000IA/LA™ Versión 092020



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



10.1 No Conformidad y Acción Correctiva

10.1.1 Cuando ocurra una no conformidad, incluida cualquiera originada por quejas, 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 y el análisis 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

10.1.1 Cuando ocurra una no conformidad, incluida cualquiera originada por quejas, la organización debe:

- c) Implementar cualquier acción necesaria.
- d) Revisar la eficacia de cualquier acción correctiva tomada.
- e) Si fuera necesario, hacer cambios en el SGS.

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

10.1.2 La organización debe conservar información documentada como evidencia de:

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



10.2 Mejora Continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de servicios.

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 que deben considerarse como parte de la mejora continua.



• • •

Anexo: Términos y Definiciones



3.1.1 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.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.2 competencia (competence): Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

3.1.3 conformidad (conformity): Cumplimiento de un requisito (3.1.19).

- **NOTA 1:** la conformidad se refiere a los requisitos de este documento, así como a los requisitos del SGS de la organización.
- **NOTA 2:** la definición del anexo SL original ha sido modificada añadiendo la NOTA 1.

3.1.4 mejora continua (continual improvement): Actividad recurrente para mejorar el desempeño (3.1.16).



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.5 acción correctiva (corrective action): acción para eliminar la causa o reducir la probabilidad de repetición de una no conformidad (3.1.12) detectada u otra situación no deseada.

- **NOTA:** se ha cambiado la definición original del anexo SL añadiendo texto a la original “acción para eliminar la causa de una no conformidad y prevenir su recurrencia”.

3.1.6 información documentada (documented information): Información que una organización (3.1.14) tiene que controlar y mantener, y el medio que la contiene.

- **EJEMPLOS:** políticas (3.1.17), planes, descripción de procesos, procedimientos (3.2.11), acuerdos de nivel de servicio (3.2.20) o contratos.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

- **NOTA 1:** la documentación puede estar en cualquier formato o medio, y puede provenir de cualquier fuente.
- **NOTA 2:** la información documentada puede hacer referencia a:
 - El sistema de gestión (3.1.9), incluidos los procesos (3.1.18) relacionados.
 - La información generada para que la organización opere (documentación).
 - La evidencia de los resultados alcanzados (registros (3.2.12)).
- **NOTA 3:** la definición original del anexo SL ha sido modificada añadiendo ejemplos.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.7 eficacia (effectiveness): grado en el que se realizan las actividades planificadas y se logran los resultados planificados.

3.1.8 parte interesada (interested party): persona u organización (3.1.14) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad relacionada con el SGS (3.2.23) o los servicios (3.2.15).

- **NOTA 1:** una parte interesada puede ser externa o interna a la organización.
- **NOTA 2:** las partes interesadas pueden incluir partes de la organización fuera del alcance del SGS, clientes (3.2.3), usuarios (3.2.28), la comunidad, proveedores externos (3.2.4), reguladores, entidades públicas, organizaciones no gubernamentales, inversores o empleados.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

- **NOTA 3:** cuando las partes interesadas se especifican en los requisitos (3.1.19) de este documento, dichas partes interesadas pueden diferir según el contexto del requisito.
- **NOTA 4:** la definición original del anexo SL ha sido modificada eliminando el término “stakeholder”, añadiendo “relacionada con el SGS o los servicios” a la definición y las Notas adicionales 1, 2 y 3.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.9 sistema de gestión (management system): conjunto de elementos de una organización (3.1.14) interrelacionados o que interactúan para establecer políticas (3.1.17), objetivos (3.1.13) y procesos (3.1.18) para lograr estos objetivos.

- **NOTA 1:** un sistema de gestión puede tratar una sola disciplina o varias disciplinas.
- **NOTA 2:** los elementos del sistema de gestión incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación, las políticas, los objetivos, los planes, los procesos y los procedimientos (3.2.11).
- **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 dentro de un grupo de organizaciones.
- **NOTA 4:** la definición original del anexo SL ha sido modificada aclarando que el sistema es un sistema de gestión y añadiendo elementos en la Nota 2.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.10 medición (measurement): proceso (3.1.18) para determinar un valor.

3.1.11 monitorización (monitoring): determinación del estado de un sistema, un proceso (3.1.18) o una actividad.

- **NOTA:** para determinar el estado puede ser necesario verificar, supervisar u observar de forma crítica.

3.1.12 no conformidad (nonconformity): incumplimiento de un requisito (3.1.19).

- **NOTA:** la no conformidad se refiere a los requisitos de este documento o a los requisitos del SGS de la organización.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.13 objetivo (objective): resultado a lograr.

- **NOTA 1:** un objetivo puede ser estratégico, táctico u operativo.
- **NOTA 2:** los objetivos pueden referirse a diferentes disciplinas [tales como financieras, de salud y seguridad, gestión de servicios (3.2.22) y ambientales] y se pueden aplicar en diferentes niveles [tales como estratégicos, para toda la organización, para servicios (3.2.15), para proyectos, productos y procesos (3.1.18)].
- **NOTA 3:** un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de gestión de servicio, o mediante el uso de términos con un significado similar (por ejemplo, propósito, finalidad o meta).
- **NOTA 4:** en el contexto de un SGS (3.2.23), la organización establece los objetivos de gestión de servicios, de forma coherente con la política (3.1.17) de gestión de servicios, para lograr resultados específicos.
- **NOTA 5:** la definición original del anexo SL ha sido modificada añadiendo “gestión de servicios” y “servicios” a la Nota 2.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.14 organización (organization): persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus objetivos (3.1.13).

- **NOTA 1:** el concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización benéfica o institución, o una parte o combinación de éstas, ya estén constituidas o no, públicas o privadas.
- **NOTA 2:** una organización o parte de una organización que gestiona y entrega un servicio (3.2.15) o servicios a clientes (3.2.3) internos o externos se puede identificar como proveedor de servicios (3.2.24).
- **NOTA 3:** en caso de que el alcance del SGS (3.2.23) incluyera sólo parte de una organización, el término organización en este documento se referiría solo a la parte de la organización incluida en el alcance del SGS. Cualquier otro uso del término organización está claramente señalado.
- **NOTA 4:** la definición original del anexo SL ha sido modificada añadiendo las Notas 2 y 3.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.15 contratar externamente (outsource): establecer un acuerdo mediante el cual una organización (3.1.14) externa realiza parte de una función o proceso (3.1.18) de una organización.

- **NOTA:** una organización externa está fuera del alcance del SGS sistema de gestión de servicios (3.2.23), aunque la función o proceso contratado externamente forme parte del alcance.

3.1.16 desempeño (performance): resultado medible.

- **NOTA 1:** el desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.
- **NOTA 2:** el desempeño se puede relacionar con la gestión de actividades, procesos (3.1.18), productos (servicios) (3.2.15), sistemas u organizaciones (3.1.14).
- **NOTA 3:** la definición original del anexo SL ha sido modificada añadiendo “servicios” a la Nota 2.

3.1.17 política (policy): intenciones y dirección de una organización (3.1.14), como las expresa formalmente su alta dirección (3.1.21).



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.18 proceso (process): conjunto de actividades interrelacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.

- **NOTA 1:** que el “resultado previsto” de un proceso se denomine salida, producto o servicio (3.2.15) depende del contexto de referencia.
- **NOTA 2:** las entradas de un proceso son generalmente las salidas de otros procesos y las salidas de un proceso son generalmente las entradas de otros procesos.
- **NOTA 3:** dos o más procesos en serie que se interrelacionan e interactúan pueden también considerarse como un proceso.
- **NOTA 4:** los procesos en una organización (3.1.14) generalmente se planifican y se realizan bajo condiciones controladas para entregar valor.
- **NOTA 5:** la definición original del anexo SL se ha cambiado desde “conjunto de actividades interrelacionadas o que interactúan que transforman entradas en salidas”. La definición original del anexo SL también ha sido modificada añadiendo las Notas 1, 2, 3 y 4. La definición revisada y de las Notas 1 a 4 proceden de la Norma ISO 9000:2015, 3.4.1.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.19 requisito (requirement): necesidad o expectativa establecida, generalmente implícita u obligatoria.

- **NOTA 1:** "Generalmente implícita" significa que es habitual o práctica común para la organización (3.1.14) y las partes interesadas (3.1.8), que la necesidad o expectativa bajo consideración está implícita.
- **NOTA 2:** un requisito especificado es aquel que está declarado, por ejemplo, en información documentada (3.1.16).
- **NOTA 3:** en el contexto de un SGS (3.2.23), los requisitos de servicio (3.2.26) están documentados y acordados en lugar de generalmente implícitos. También puede haber otros requisitos, como los legales o regulatorios.
- **NOTA 4:** la definición original del anexo SL ha sido modificada añadiendo la Nota 3.



3.1 Términos Específicos a las Normas de Sistemas de Gestión

3.1.20 riesgo (risk): efecto de la incertidumbre.

- **NOTA 1:** un efecto es una desviación de lo esperado, ya sea positivo o negativo.
- **NOTA 2:** incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o su probabilidad.
- **NOTA 3:** con frecuencia el riesgo se caracteriza por referencia potenciales (según se define en la Guía ISO 73:2009, 3.5.1.3) consecuencias" (según se define en la Guía ISO 73:2009, 3.6.1.3), o a una combinación de éstos.
- **NOTA 4:** con frecuencia el riesgo se expresa en términos de una combinación de las consecuencias de un evento (incluidos cambios en las circunstancias) y la "probabilidad" (según se define en la Guía ISO 73:2009, 3.6.1.1) asociada de que ocurra.

3.1.21 alta dirección (top management): Persona o grupo de personas que dirige y controla una organización (3.1.14) al más alto nivel.

- **NOTA 1:** la alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.
- **NOTA 2:** si el alcance del sistema de gestión (3.1.9) comprende sólo una parte de una organización, entonces "alta dirección" se refiere a quienes dirigen y controlan esa parte de la organización.



3.2 Términos Específicos a la Gestión de Servicios

3.2.1 activo (asset): elemento, cosa o entidad que tiene valor potencial o real para una organización (3.1.14).

- **NOTA 1:** el valor puede ser tangible o intangible, financiero o no financiero, e incluye la consideración de riesgos (3.1.20) y obligaciones. Puede ser positivo o negativo en diferentes etapas de la vida del activo.
- **NOTA 2:** los activos físicos generalmente se refieren a equipos, inventario y propiedades que posee la organización. Los activos físicos son lo opuesto a los activos intangibles, que son activos no físicos tales como alquileres, marcas, activos digitales, derechos de uso, licencias, derechos de propiedad intelectual, reputación o acuerdos.
- **NOTA 3:** una agrupación de activos que se conoce como un sistema de activos también podría considerarse como un activo.
- **NOTA 4:** un activo también puede ser un elemento de configuración (3.2.2). Algunos elementos de configuración no son activos.

[FUENTE: ISO/IEC 19770-5:2015, 3.2, modificado – La Nota 4 incluye contenido nuevo].



3.2 Términos Específicos a la Gestión de Servicios

3.2.2 elemento de configuración, CI (configuration item): elemento que es necesario controlar para proveer uno o varios servicios (3.2.15).

3.2.3 cliente (customer): organización (3.1.14) o parte de una organización que recibe uno o varios servicios (3.2.15).

- **EJEMPLOS:** consumidor, cliente, beneficiario, patrocinador y comprador.
- **NOTA 1:** un cliente puede ser interno o externo a la organización que entrega el servicio o servicios.
- **NOTA 2:** un cliente también puede ser usuario (3.2.28). Un cliente también puede actuar como proveedor.

3.2.4 proveedor externo (external supplier): parte externa a la organización que suscribe un contrato para contribuir a la planificación, diseño, transición (3.2.27), entrega o mejora de un servicio (3.2.15), componente de un servicio (3.2.18) o proceso (3.1.18).

- **NOTA 1:** Los proveedores externos incluyen proveedores principales designados, pero no sus proveedores subcontratados.
- **NOTA 2:** Si la organización en el alcance del SMS es parte de una organización mayor, la parte externa lo es de la organización mayor.



3.2 Términos Específicos a la Gestión de Servicios

3.2.5 incidencia (incident): una interrupción inesperada de un servicio (3.2.15), una reducción en la calidad de un servicio o un evento que todavía no ha tenido impacto en el servicio para el cliente (3.2.3) o para el usuario (3.2.28).

3.2.6 seguridad de la información (information security): la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **NOTA:** Además, pueden estar involucradas otras propiedades como autenticidad, trazabilidad, no repudio y fiabilidad.

[FUENTE: ISO/IEC 27000:2018, 3.28].

3.2.7 incidencia de seguridad de la información (information security incident): un único evento o una serie de eventos de seguridad de la información (3.2.6) inesperados o no deseados, que tienen una significativa probabilidad de comprometer las operaciones del negocio y de amenazar la seguridad de la información.

[FUENTE: ISO/IEC 27000:2018, 3.31].



3.2 Términos Específicos a la Gestión de Servicios

3.2.8 proveedor interno (internal supplier): parte de una organización (3.1.14) mayor, que está fuera del alcance del SGS (3.2.23) que suscribe un acuerdo documentado para contribuir a la planificación, diseño, transición (3.2.27), entrega o mejora de un servicio (3.2.15), componente de servicio (3.2.18) o proceso (3.1.18).

- **EJEMPLO:** adquisiciones, infraestructura, finanzas, recursos humanos, instalaciones.
- **NOTA:** el proveedor interno y la organización en el alcance del SGS deben ser ambos parte de la misma organización mayor.

3.2.9 error conocido (known error): problema (3.2.10) que tiene identificados una causa raíz o un método para reducir o eliminar su impacto sobre un servicio (3.2.15).

3.2.10 problema (problem): causa de una o más incidencias (3.2.5) reales o potenciales.

3.2.11 procedimiento (procedure): forma especificada de llevar a cabo una actividad o un proceso (3.1.18).

- **NOTA:** los procedimientos pueden ser documentados o no.

[FUENTE: ISO 9000:2015, 3.4.5].



3.2 Términos Específicos a la Gestión de Servicios

3.2.12 registro (record): documento que presenta resultados obtenidos o proporciona evidencia de actividades realizadas.

- **EJEMPLOS:** informes de auditoría (3.1.1), datos de una incidencia (3.2.5), listado de asistentes a formaciones o actas de reuniones.
- **NOTA 1:** los registros pueden utilizarse, por ejemplo, para formalizar la trazabilidad y para proporcionar evidencia de verificaciones, acciones preventivas y acciones correctivas (3.1.5).
- **NOTA 2:** en general, los registros no necesitan estar sujetos al control de revisión.

[FUENTE: ISO 9000:2015, 3.8.10, modificado – Se ha añadido el EJEMPLO].

3.2.13 entrega (release): fecopilación de uno o más servicios (3.2.15) nuevos o modificados, o de componentes de servicio (3.2.18), desplegados en el entorno de producción como resultado de uno o más cambios.



3.2 Términos Específicos a la Gestión de Servicios

3.2.14 petición de cambio (request for change): propuesta de modificación a aplicar a un servicio (3.2.15), a un componente de un servicio (3.2.18) o al SGS (3.2.23).

- **NOTA:** un cambio a un servicio incluye la entrega de un servicio nuevo, la transferencia de un servicio o la retirada de un servicio que ya no es necesario.

3.2.15 servicio (service): medio de entrega de valor al cliente (3.2.3) facilitándole los resultados que quiere lograr.

- **NOTA 1:** el servicio es generalmente intangible.
- **NOTA 2:** el término servicio de acuerdo a este documento se refiere al servicio o servicios dentro del alcance del SGS (3.2.23). Cualquier uso del término servicio con un propósito diferente se distingue claramente.



3.2 Términos Específicos a la Gestión de Servicios

3.2.16 disponibilidad de servicio (service availability): capacidad de un servicio (3.2.15), o componente de servicio (3.2.18), de realizar la función requerida en un momento acordado o durante un periodo de tiempo acordado.

- **NOTA:** la disponibilidad puede expresarse como un ratio o porcentaje de tiempo en el que el servicio o componente del servicio está realmente disponible para su uso en relación con el tiempo acordado.

3.2.17 catálogo de servicios (service catalogue): información documentada sobre los servicios que una organización proporciona a sus clientes.

3.2.18 componente de servicio (service component): parte de un servicio (3.2.15) que cuando se combina con otros elementos provee un servicio completo.

- **EJEMPLOS:** Infraestructura, aplicaciones, documentación, licencias, información, recursos, servicios de soporte.
- **NOTA:** Un componente de servicio puede incluir elementos de configuración (3.2.2), activos (3.2.1) u otros elementos.



3.2 Términos Específicos a la Gestión de Servicios

3.2.19 continuidad de los servicios (service continuity): capacidad de entregar un servicio (3.2.15) sin interrupción, o con disponibilidad constante según lo acordado.

- **NOTA:** la gestión de la continuidad de los servicios puede ser un subconjunto de la gestión de la continuidad del negocio. La Norma ISO 22301 es una norma para la implementación de un sistema de gestión de la continuidad del negocio.

3.2.20 acuerdo de nivel de servicio, SLA (service level agreement): acuerdo documentado entre la organización (3.1.14) y el cliente (3.2.3) que identifica los servicios (3.2.15) y su rendimiento acordado.

- **NOTA 1:** un acuerdo de nivel de servicio puede también establecerse entre la organización y un proveedor externo (3.2.4), un proveedor interno (3.2.8) o un cliente actuando como proveedor.
- **NOTA 2:** un acuerdo de nivel de servicio puede ser incluido en un contrato u otro tipo de acuerdo documentado.

3.2.21 objetivo de nivel de servicio (service level target): Característica específica medible de un servicio (3.2.15) a la que la organización (3.1.14) se compromete.



3.2 Términos Específicos a la Gestión de Servicios

3.2.22 gestión de servicios (service management): conjunto de capacidades y procesos (3.1.18) para dirigir y controlar las actividades y recursos de la organización (3.1.14) para la planificación, diseño, transición (3.2.27), entrega y mejora de los servicios (3.2.15) con la finalidad de entregar valor (3.2.29).

- **NOTA:** este documento proporciona un conjunto de requisitos que se dividen en capítulos y apartados. Cada organización puede elegir cómo combinar los requisitos en los procesos. Los apartados pueden usarse para definir los procesos del SGS de la organización.

3.2.23 sistema de gestión de servicios, SGS (service management system): Sistema de gestión (3.1.9) para dirigir y controlar las actividades de gestión de los servicios (3.2.22) de la organización (3.1.14).

- **NOTA:** el SGS incluye las políticas (3.1.17), los objetivos (3.1.13), los planes, los procesos (3.1.18) y la información documentada de la gestión de servicios, así como los recursos requeridos para la planificación, diseño, transición (3.2.27), entrega y mejora de los servicios con la finalidad de cumplir con los requisitos (3.1.19) especificados en este documento.



3.2 Términos Específicos a la Gestión de Servicios

3.2.24 proveedor de servicio (service provider): organización (3.1.14) que gestiona y provee uno o varios servicios (3.2.15) a clientes (3.2.3).

3.2.25 petición de servicio (service request): solicitud de información, consulta, de acceso a un servicio (3.2.15) o un cambio previamente aprobado.

3.2.26 requisitos de servicio (service requirement): necesidades de los clientes (3.2.3), los usuarios (3.2.28) y la organización (3.1.14) relacionados con los servicios (3.2.15) y el SGS (3.2.23) que han sido enunciadas o son obligatorias.

- **NOTA:** en el contexto de un SGS (3.2.23), los requisitos de servicio están documentados y acordados en lugar de estar generalmente implícitos. También pueden existir otros requisitos, tales como requisitos legales y regulatorios.



3.2 Términos Específicos a la Gestión de Servicios

3.2.27 transición (transition): actividades involucradas en el traslado de un servicio (3.2.15) nuevo o modificado desde o hasta el entorno de producción.

3.2.28 usuario (user): individuo o grupo que interactúa o se beneficia de un servicio (3.2.15) o servicios.

- **NOTA:** Los ejemplos de usuarios incluyen una persona o comunidad de personas. Un cliente (3.2.3) también puede ser un usuario.

3.2.29 valor (value): importancia, beneficio o utilidad.

- **EJEMPLO:** valor monetario, logro de resultados de servicio, consecución de los objetivos (3.1.13) de la gestión de servicios (3.2.22), retención de clientes, eliminación de restricciones.
- **NOTA:** la creación de valor a partir de los servicios (3.2.15) incluye la obtención de beneficios a un nivel óptimo de recursos gestionando el riesgo (3.1.20). Un activo (3.2.1) y un servicio (3.2.15) son ejemplos a los que se puede asignar un valor.



• • •

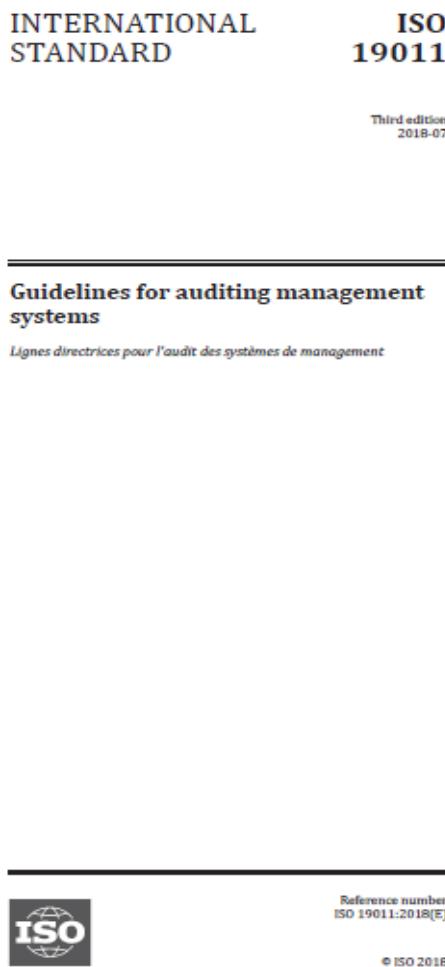
11. Módulo de Auditoría ISO 19011



I20000IA/LA™ Versión 092020



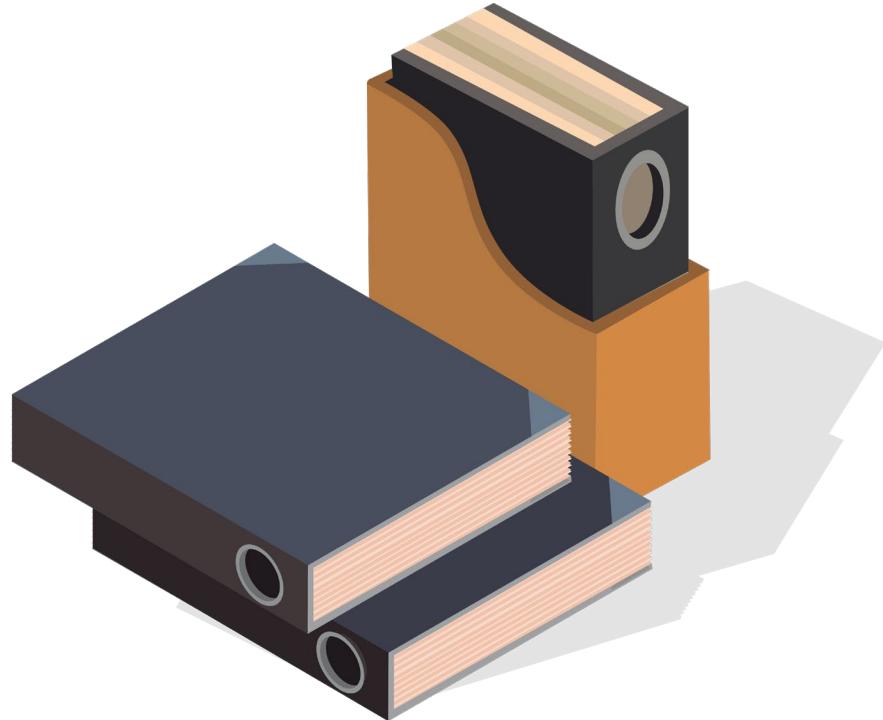
ISO 19011:2018



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.

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.

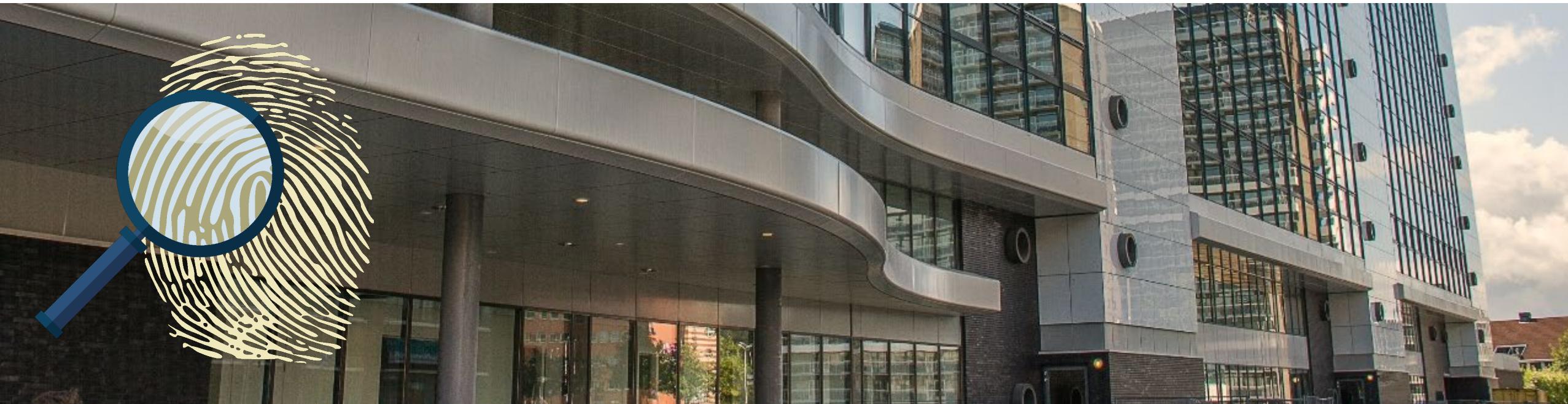
Cliente de la Auditoría



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 en su totalidad o partes de ella siendo auditada.

Auditor



Persona que realiza 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.

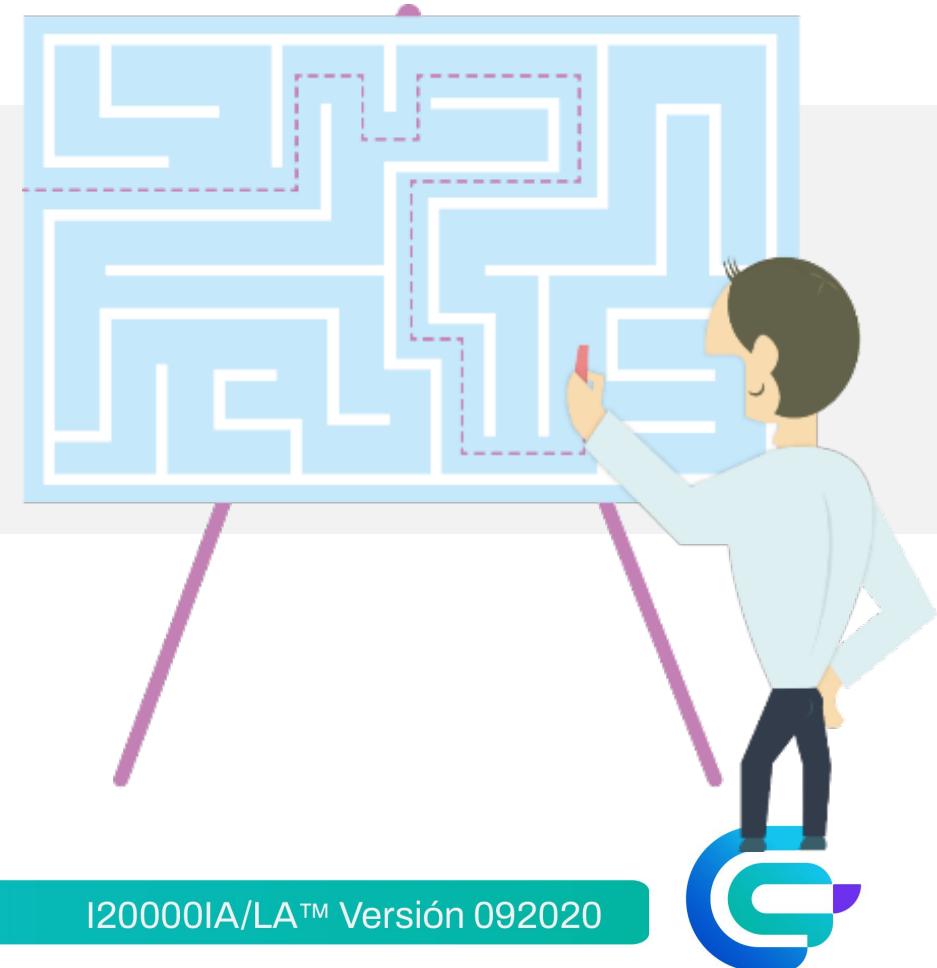
Nota 2: un experto técnico del equipo de auditoría no actúa como auditor.

Observador



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

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.

Planeación



Descripción de las actividades y los arreglos para 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.

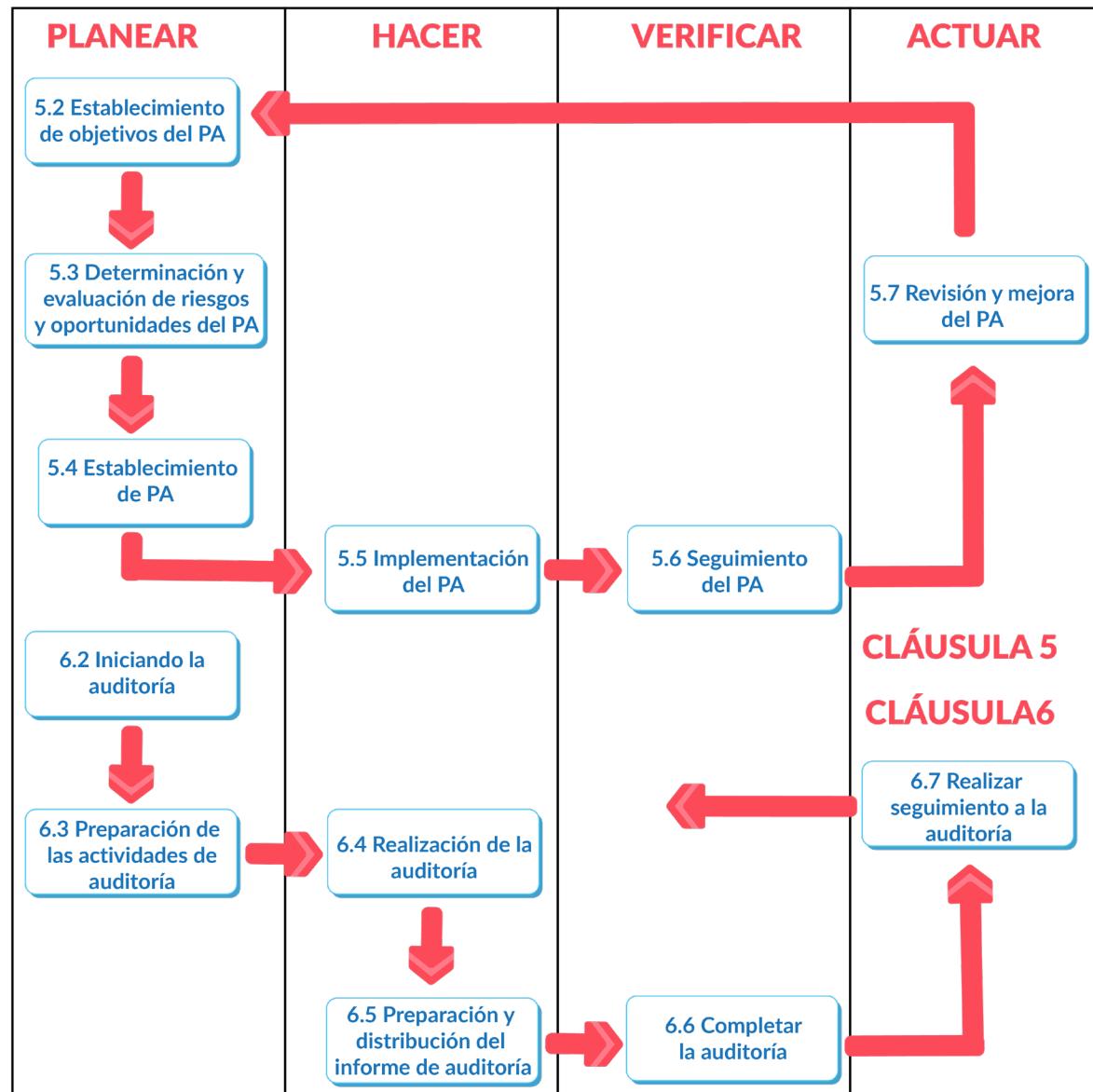
El alcance de un programa de auditoría debería basarse en el tamaño y la naturaleza del auditado, así como en la naturaleza, funcionalidad, complejidad, el tipo de riesgos y oportunidades, y el nivel de madurez de los sistemas de gestión a ser auditados.

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/subcláusulas 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.



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.

01

02

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.

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.

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/proveer 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.
- Audituar 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 muestrada.



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(os) 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 1



Taller 1: Elaborar Plan de Auditoría.

Taller 2



Taller 2: 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 3



Taller 3: Elaborar una lista de verificación para auditar las cláusulas 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.

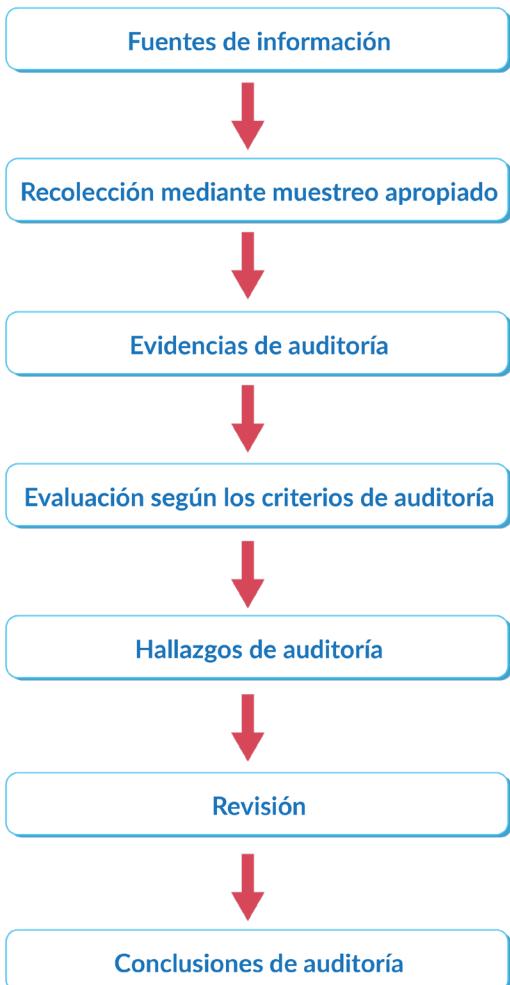


Métodos para Recopilar Información

- 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 límite de tiempo y cumplirlo.
- Ser creativo.

Manejo de Situaciones Difíciles

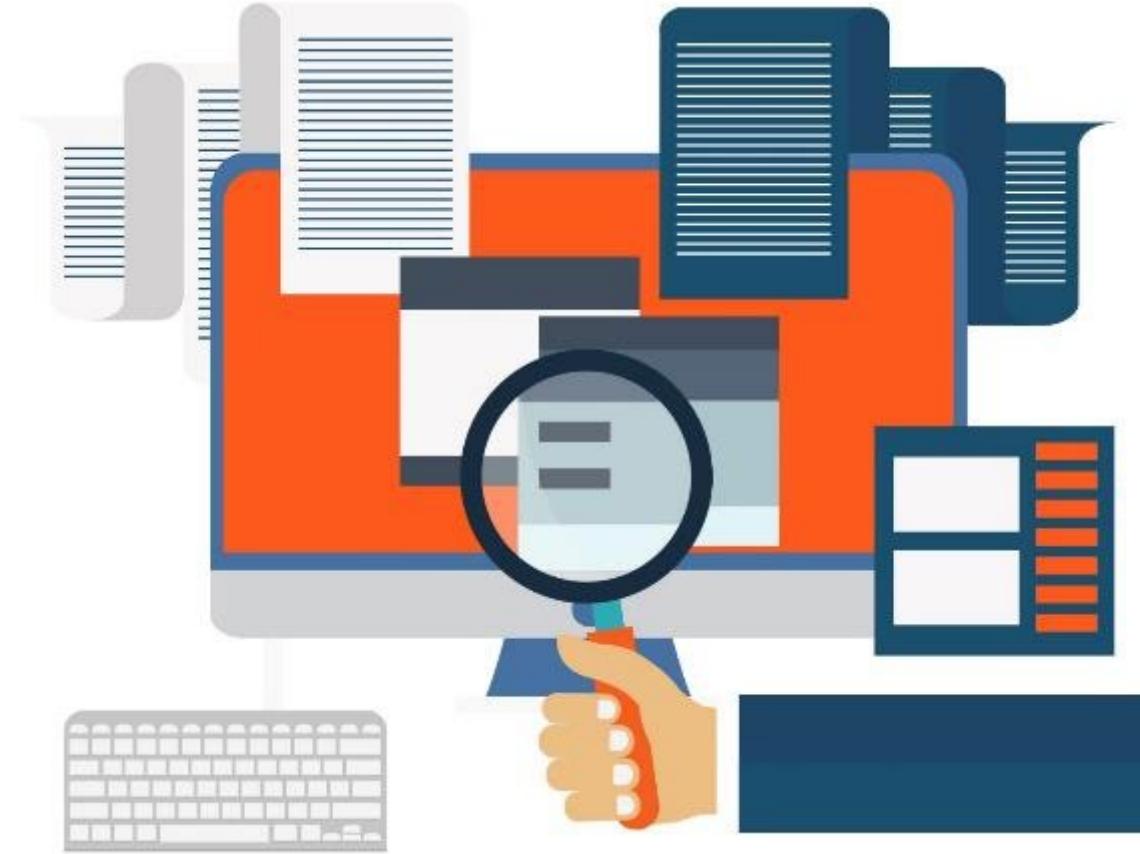
- A la reunión de apertura no se presenta el responsable del proceso o actividad auditada.
- En la auditoría se tenía previsto visitar dos instalaciones y no hay disponibles vehículos, ni acompañantes.
- El auditado desvía la pregunta del auditor. Ejemplo: pregunta por la forma como se controlan los 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 4



Taller 4: Según el formato, realizar el informe de auditoría.



¡Síguenos, ponte en contacto!



www.certiprof.com

CERTIPROF® is a registered trademark of Certiprof,
LLC in the United States and/or other countries.