1.- OBJETIVO

Este documento describe las actividades y la metodología para otorgar, negar, mantener, ampliar o reducir el alcance, renovar, suspender o restaurar, o retirar las certificaciones de Sistemas de Gestión de ASOCIACIÓN CIVIL BASC PERÚ; de acuerdo con lo establecido en la norma ISO 17021-1:2015 “Evaluación de la Conformidad. Requisitos para los organismos que realizan auditoría y Certificación de Sistemas de Gestión” y la norma ISO/IEC 27006:2015 Tecnología de la información - Técnicas de seguridad – Requisitos para entidades que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información.

2.- ALCANCE

El presente procedimiento es de obligatorio cumplimiento para todo el personal que intervienen en los procesos de certificación de las normas ISO que ASOCIACIÓN CIVIL BASC PERÚ disponga.

3.- REFERENCIAS

a. DOCUMENTOS EXTERNOS. - Los criterios tomados en cuenta para la elaboración y aplicación del presente documento son las siguientes normas y documentos de origen externo:

(1) Norma ISO 17000 Evaluación de conformidad - Vocabulario y principios generales.

(2) Norma ISO 17021-1:2015 Evaluación de la conformidad. Requisitos para los organismos que realizan a auditoría y la certificación de sistemas de gestión. Parte 1: Requisitos

(3) IAF MD 1:2023. Documento obligatorio de IAF para la Certificación Multi-sitio Basada en el Muestreo.

(4) IAF MD 2:2023. Transferencia de sistemas de gestión de certificación acreditados. Documento obligatorio para el MLA de IAAC de certificación de sistemas de gestión

(5) IAF MD 4:2023. Documento obligatorio de la IAF para el uso de las tecnologías de la información y la comunicación (TIC) con fines de auditoría / evaluación. Documento obligatorio para el MLA de IAAC de certificación de sistemas de gestión.

(6) IAF MD 5:2023. Determinación del tiempo de auditoría de sistemas de gestión de calidad, ambiental y seguridad y salud en el trabajo.

(7) Documento obligatorio para el MLA de IAAC de certificación de QMS y EMS.

(8) IAF MD 7:2023. Documento obligatorio de IAF para la armonización de sanciones a ser aplicadas a organismos de evaluación de la conformidad. Documento obligatorio para el MLA de IAAC de certificación.

(9) IAF MD11:2023. Aplicación de la ISO/IEC 17021 para auditorías de Sistemas de Gestión Integrados (IMS). Documento obligatorio para el MLA de IAAC de certificación de sistemas de gestión.

(10) IAF MD17:2023 Actividades de testificación para la acreditación de organismos de certificación de sistemas de gestión

(11) ISO / IEC TS 17021-3:2017 Requisitos de competencia para la auditoría y la certificación de sistemas de gestión de la calidad

(12) ISO / IEC TS 17021-9:2016 Requisitos de competencia para la auditoría y la certificación de sistemas de gestión antisoborno

(13) ISO/IEC 17021-13: 2021 Requisitos de competencia para la auditoría y la certificación de sistemas de gestión del compliance

(14) IAF- ID 1:2023 Documento informativo de la IAF para los alcances de acreditación de QMS y EMS

(15) IAF-ID3:2011 Documento informativo para la gestión de eventos extraordinarios o circunstancias que afecten a ABs, CABs y organizaciones certificadas

(16) IAF- ID12:2023 Principios sobre evaluación remota

(17) IAF ID14:2023 Guía sobre la determinación del tiempo de auditoría para la auditoría integrada de sistemas de gestión de múltiples sitios

(18) Anexo A de ISO/IEC 17021-1:2015 EVALUACION DE LA CONFORMIDAD – requisitos para los organismos que realizan la auditoria y la certificacion de sistemas de gestion – parte 1: requisitos

b. DOCUMENTOS INTERNOS. - Se hace referencia a ciertos documentos dentro del Sistema Integrado de Gestión, que se deben aplicar al momento de desarrollar las actividades del procedimiento:

(1) Procedimiento Comunicaciones con el Asociado y no Asociado (P-COM-001)

(2) Procedimiento Percepción del Cliente (P-COM-002)

(3) Procedimiento Quejas y Sugerencias (P-COM-003)

(4) Procedimiento Gestión de Apelaciones (P-CISO-002)

(5) Procedimiento Selección, Contratación y Evaluación de Auditores y Expertos Técnicos (P-CISO-003)

(6) Procedimiento Gestión de Auditorías Remotas (P-CISO-007)

(7) Procedimiento Gestión de las Comunicaciones (P-CISO-009)

(8) Reglamento para el uso de Marcas de Certificación ISO (D-CISO-006)

(9) Documento de Apoyo Auditor (D-CISO-011)

(10) Tarifa de Certificación ISO (D-CISO-039)

4.- DEFINICIONES

a. Para efectos de este procedimiento se aplicarán los términos y definiciones establecidos en la ISO/IEC 17000:2020 Evaluación de conformidad - Vocabulario y principios generales.

b. Los términos y definiciones usadas en este procedimiento son:

(1) Evaluación de la Conformidad: Demostración de que se cumplen los requisitos específicos relativos a un producto, proceso, sistema, persona u organismo.

(2) Apelación: Solicitud del proveedor del objeto de evaluación de conformidad al organismo de evaluación de la conformidad o al organismo de acreditación, de reconsiderar la desición que tomó en relación con dicho objeto.

(3) Queja: Expresión de insatisfacción, diferente de la apelación, presentada por una persona u organización a un organismo de evaluación de la conformidad o a un organismo de acreditación, relacionada con las actividades de dicho organismo, para la que se espera una respuesta.

(4) Cliente Certificado: La organización cuyo sistema de gestión se ha certificado.

(5) Guía: Persona designada por el cliente para asistir al equipo auditor. Las personas guías se asignan al equipo auditor para facilitar la auditoría.

(6) Imparcialidad: Presencia real y percibida de objetividad.

(7) Observador: Persona que acompaña al equipo auditor, pero no audita, un observador no es parte del equipo auditor y no influye o interfiere con la realización de la auditoría.

(8) Sitio: Un sitio es un lugar permanente donde una organización realiza su trabajo o servicio.

(9) Sitio Temporal: Un sitio temporal es aquél establecido por una organización para desempeñar un trabajo específico o un servicio por un período de tiempo finito, y que no se convertirá en un lugar permanente. (por ejemplo: sitio de construcción).

(10) Sitios Adicionales: Un sitio nuevo o grupo de sitios que serán agregados a una red de multi-sitios certificados.

(11) Multisitio: Una organización multi-sitio se define como una organización que cuenta con una función central identificada (de aquí en adelante nombrado como una oficina central – pero no necesariamente la oficina principal de la organización), en donde se planean, controlan o gestionan ciertas actividades, y una red de oficinas locales o sucursales (sitios) en donde tales actividades se llevan a cabo de forma total o parcial.

5.- RESPONSABLE

El Gerente de Operaciones de ASOCIACIÓN CIVIL BASC PERÚ es el responsable del seguimiento a la aplicación de este procedimiento.

6.- DESARROLLO

a. ATENCION DE LA SOLICITUD DE CERTIFICACIÓN / RE-CERTIFICACIÓN

(1) Recepción de la Solicitud[1]

(a) El área de Afiliaciones y Servicios Especializados de ASOCIACIÓN CIVIL BASC PERÚ es el encargado de atender las solicitudes de Certificación, **Renovación y Transferencia** de los clientes; **el área de Sistema Integrado de Gestión y Proyectos será el responsable de atender las solicitudes de Seguimiento**. Toda la información concerniente al proceso de certificación está incluido en el formato de solicitud que se encuentra disponible en la página web: www.bascperu.org[3]

(b) Cuando sea aplicable y el cliente lo requiera, la información concerniente a la solicitud de certificación se le hará llegar vía correo electrónico o se le informará personalmente en las instalaciones de ASOCIACIÓN CIVIL BASC PERÚ o en las instalaciones del cliente.

(c) La solicitud formal por parte de un cliente se realiza a través del formato “Solicitud de Certificación, Seguimiento o Renovación” (F-CISO-001) el cual se debe hacer llegar al área según corresponda con la información que solicita el registro, el cual permitirá evidenciar la implementación del Sistema de Gestión y determinar los tiempos de auditoría. Sólo para los casos en que la solicitud de auditoría de certificación o renovación sea en la Norma ISO 37001:2016, en adición al formato de solicitud, el cliente del sector privado deberá completar y firmar el cuestionario externo de debida diligencia a terceros (F-CISO-004), el cual será revisado por la Gerencia de Afiliaciones y Fidelización, así como por la Gerencia de Operaciones y

[1] Norma ISO 17021-1 cláusula 9.1.1.- Actividad previa a la certificación - Solicitud
[2] Norma ISO 17021-1 cláusula 8.- Requisitos relativos a la información.
[3] Norma ISO 17021-1 cláusula 8.- Requisitos relativos a la información.

aprobación de la Gerencia General. En caso de ausencia de alguno de los miembros, se continuará con las revisiones de aprobación según corresponda.

(d) Este formato aplica para procesos de Certificación, Seguimiento, Transferencia, Renovación y ampliación de alcance. Contiene la siguiente información:

1 El alcance deseado de la certificación.
2 Las características generales de la organización solicitante, tal y como se requiera por el esquema de certificación específico, incluido el nombre y las direcciones de sus ubicaciones físicas, sus procesos y operaciones, recursos humanos y técnicos, funciones, relaciones y cualquier obligación legal pertinente;
3 La identificación de procesos contratados externamente utilizados por la organización que afectarán a la conformidad con los requisitos;
4 Las normas u otros requisitos para los cuales la organización solicitante pide la certificación;
5 Si se ha presentado consultoría relacionada con el sistema de gestión que se va a certificar, así como, quién la proporcionó.
6 Otras certificaciones con las que cuente la organización.
7 Evidencias de documentación del Sistema de Gestión, a presentarse con la aceptación de la propuesta de certificación.

(2) Revisión de la Solicitud[4]

(a) El área **responsable** revisa la solicitud de la certificación, **seguimiento o renovación** verificando que ésta cumpla con los requisitos definidos en este procedimiento.

(b) Aspectos como, el alcance de la certificación del Sistema de Gestión debe ser claro, preciso y objetivo en términos del servicio a certificar, de no ser así ASOCIACIÓN CIVIL BASC PERÚ podrá proponer modificaciones al mismo. El alcance de certificación deberá establecer los sitios donde se realizan las actividades objeto de la empresa con el fin de realizar la planeación de la auditoría de certificación bajo el enfoque de Multi-sitio (IAF MD1) o combinada (IAF MD11).

(c) Antes de proceder a formular la propuesta, el organismo de certificación a través de la “Jefatura de SIG y Proyectos” y “Gerencia de Afiliaciones y Fidelización” lleva a cabo una revisión de la solicitud y de la información complementaria para la certificación a fin de asegurar que:

1 La información relativa a la organización solicitante y a su sistema de gestión son suficientes para llevar a cabo la auditoría.
2 Los requisitos de la certificación están claramente definidos y documentados y se han proporcionado a la organización solicitante.
3 Se ha resuelto cualquier diferencia de entendimiento entre el organismo de certificación y la organización solicitante.

[4] Norma ISO 17021-1 cláusula 9.1.1.- Actividad previa a la certificación – Revisión de la solicitud

4 El organismo de certificación tiene la competencia (acreditación, Código IAF, equipo auditor calificado para lo cual verifica la información de la Matriz de Clasificación Sectorial F-CISO-003).

5 El organismo de certificación tiene la capacidad para llevar a cabo la actividad de certificación. Se tienen en cuenta el alcance de la certificación solicitada, las ubicaciones donde la organización solicitante lleva a cabo sus actividades, el tiempo requerido para completar las auditorías y cualquier otro asunto que tenga influencia sobre la actividad de certificación (idioma, condiciones de seguridad, amenazas a la imparcialidad, etc.).

(d) Identificación de problemas en la solicitud de información complementaria.

1 Cuando existan inconsistencias o falta de claridad en el proceso de solicitud del servicio, ASOCIACIÓN CIVIL BASC PERÚ solicitará formalmente a través de correo electrónico, o algún medio de comunicación al cliente, la aclaración respectiva hasta tanto se complete la documentación o información requerida.

2 El proceso de solicitud no se da por finalizado hasta que no exista seguridad en las partes sobre la aclaración de dudas y requerimientos.

(e) Respuesta de Solicitud al Cliente

1 La respuesta al cliente tendrá un tiempo máximo de diez (10) días hábiles de aceptación **en la medida de lo posible.**

2 Después de la revisión de la solicitud, ASOCIACIÓN CIVIL BASC PERÚ a través del área **correspondiente** informa al Cliente de auditoría sobre la aceptación o rechazo de la solicitud de certificación. Una empresa podrá ser rechazada por observaciones encontradas en la verificación de antecedentes, por no contar con licencia de funcionamiento (salvo excepciones) o cualquier otra razón indicada por la alta dirección

3 De ser rechazada la solicitud de certificación, ASOCIACIÓN CIVIL BASC PERÚ a través del área **correspondiente** documentará las razones y las indicará al Cliente de auditoría. La actuación en estos casos por parte de ASOCIACIÓN CIVIL BASC PERÚ se realizará atendiendo los principios de imparcialidad, competencia, responsabilidad, transparencia, confidencialidad y receptividad y respuesta oportuna a las quejas manejadas por ASOCIACIÓN CIVIL BASC PERÚ como organismo evaluador de la conformidad.

4 ASOCIACIÓN CIVIL BASC PERÚ mantendrá los registros de la justificación sobre la decisión de llevar a cabo la certificación mediante “Formato de solicitud Certificación/Renovación” (F-CISO-001) en el acápite denominado espacio para uso exclusivo de ASOCIACIÓN CIVIL BASC PERÚ.

5 El área de Afiliaciones y Fidelización y el área de Sistema Integrado de Gestión y Proyectos elaborarán la Propuesta de Certificación, Seguimiento o Renovación (F-CISO-005), según corresponda, considerando previamente:

a **Elabora el registro de Determinación de Tiempos (F-CISO-014) tomando como base lo establecido en los Anexos A hasta el G, que establece Generalidades, Guías para Determinación de los Tiempos de Auditoría, según la norma certificable y reducción y ampliación de tiempos.** [5]

b **Establece los costos del servicio, de acuerdo a las Tarifas de Certificación ISO (D-CISO-039).**

c **En caso de que un cliente solicite un proceso de auditoría de certificación continuada, es decir al culminar la Etapa 1 al día siguiente se inicia la Etapa 2, deberá indicarse al cliente ya sea por medio digital (email) o una carta, que los riesgos de realizar una auditoría continuada podrían ser:**

1º Información proporcionada en la Solicitud de certificación no corresponde al Sistema de Gestión, tal como, número de personal, ubicaciones del cliente, procesos, equipos, nivel de control en caso multi-sitio y requisitos legales y reglamentación.

2º Hallazgos de No conformidades y tiempo para implementar el plan de acción pertinente.

3º Recursos insuficientes para llevar a cabo la Etapa 2.

Por tanto, la Etapa 2 no podría llevarse a cabo y tendría que reprogramarse con el cargo de una penalidad al cliente.

6 La Propuesta de Certificación, **Seguimiento o Renovación** (F-CISO-005) **será revisada por la Gerencia de Operaciones y aprobada por la Gerencia General**, en caso de ausencia de alguno de los miembros, se continuará con las revisiones de aprobación según corresponda. Se entrega al cliente junto con el Acuerdo de Certificación (F-CISO-006) [6-7]; si el cliente acepta la propuesta, deberá firmar en señal de aprobación dichos documentos y los hará llegar por medio electrónico al área que corresponda.

7 Una vez que se cuente con la constancia de pago, la Propuesta de Certificación (F-CISO-005), el Acuerdo de Certificación (F-CISO-006) firmados y los documentos anexos requeridos en la Solicitud, se procederá con la siguiente etapa.

b. PLANEACIÓN DE AUDITORÍA

(1) Desarrollo del Programa de Auditoría[8]

[5] Norma ISO 17021-1 cláusula 9.1.4.- Determinación de tiempos de auditoría / 9.1.5.- Muestreo multisitio y 9.1.6.- Sistema de gestión múltiples
[6] Norma ISO 17021-1 Cláusula 5.1.2. Acuerdo de certificación.
[7] Norma ISO 17021-1 Cláusula 8.5 Intercambio de información entre el organismo de certificación y sus clientes.
[8] Norma ISO 17021-1 cláusula 9.1.3.- Programa de Auditoría

(a) El área de SIG debe asegurar que el auditor de certificación (Etapa 1 y 2) elabore un Programa de Auditorías ISO por empresa para el ciclo completo de su certificación, a fin de identificar claramente las actividades de auditoría que se requieren para verificar que el sistema de gestión cumple los requisitos de certificación.

(b) El programa de auditoría incluye una auditoría inicial en dos etapas, auditorías de seguimiento en el primer y segundo año y una auditoría de renovación de la certificación en el tercer año, antes de la caducidad de la certificación. El periodo de certificación de tres (03) años comienza con la decisión de certificación o de renovación de la certificación.

(c) La determinación del programa de auditoría y cualquier modificación subsiguiente debe tener en cuenta el tamaño de la organización del cliente, el alcance, los turnos de trabajo, la complejidad de su sistema de gestión, los productos y procesos, así como el nivel demostrado de eficacia del sistema de gestión y los resultados de auditorías previas.

(d) El programa de auditoría puede tener ajustes a partir de la identificación de otras certificaciones ya otorgadas, otras auditorías ya realizadas al cliente o resultados de la Etapa 2, lo que se soportará con evidencias para la justificación del ajuste. Asimismo, la coordinación con el Cliente sobre las fechas de auditoría, pueden influir en la programación.

(e) Entre la etapa 1 y etapa 2 de auditoría no debe existir un tiempo mayor a seis (06) meses.

(f) Los plazos establecidos en el presente procedimiento no pueden extenderse bajo ningún motivo o excusa. La auditoría del primer seguimiento tiene plazo de un (01) año desde la fecha de decisión de certificación, a excepción de la auditoría de seguimiento 2 y la renovación, antes de culminar la vigencia del certificado actual.

(g) La determinación del programa de auditoría y cualquier ajuste posterior deberán tener en cuenta el tamaño del cliente, el alcance y la complejidad de su sistema de gestión, productos y procesos, así como el nivel demostrado de eficacia del sistema de gestión y los resultados de auditorías anteriores. Puede ser necesario ajustar la frecuencia de las auditorías de vigilancia para adaptarse a factores como las estaciones del año o la certificación de sistemas de gestión de duración limitada (por ejemplo, una obra de construcción temporal).

(2) Planificación de Auditoría

(a) Determinación de los Objetivos, Alcance y Criterios de la Auditoría[9]

Los objetivos, alcance y criterios de la auditoría se definen en el Plan de Auditoría (F-CISO-012).

[9] Norma ISO 17021-1, cláusula 9.2.1.- Determinación de objetivos, alcance y criterios de auditoría.

(b) Selección del equipo auditor, personal de apoyo y observadores [10]

1 El personal que compone el staff de auditores de certificación es previamente calificado por la ASOCIACIÓN CIVIL BASC PERU a través de la aplicación del procedimiento Selección, Contratación y Evaluación de Auditores y Expertos Técnicos (P-CISO-003).

2 El Jefe de SIG determina el tamaño y composición del equipo auditor a partir de los siguientes criterios:

a **Los objetivos, alcance y criterios de la auditoría, y la duración estimada de la misma.**

b **Si la auditoría es combinada, integrada (con otros sistemas de gestión) o conjunta (con otros Organismos de Certificación).**

c **Los requisitos de la certificación (incluidos todos los requisitos legales, reglamentarios o contractuales aplicables)**

d **El idioma y la cultura.**

e **La competencia global del equipo auditor, necesaria para lograr los objetivos de la auditoría. Para ello:**

1º Del staff de auditores calificados, identifica la competencia y el expertise del auditor, según código IAF asignado y registrado en la Matriz de Clasificación Sectorial (F-CISO-003).

2º Se asignará respectivamente el que tenga mayor experiencia y si no se encuentra disponible continuará con el que le sigue en la Matriz, también se verifica que no exista conflicto de interés de acuerdo a la información registrada en la Matriz Auditores y Consultorías (F-CISO-018).

3º Soportado en competencias se designa al líder del equipo auditor.

4º Si dentro del staff de auditores no se contara con las competencias, se deberá considerar la lista de expertos técnicos competentes, según el código IAF que se requiera auditar.

5° **Para auditorías en ISO/IEC 27001 se considerará el formato F-CISO-041 Sectores y áreas técnicas.**

f **Si los miembros del equipo auditor han auditado previamente el sistema de gestión del cliente.**

g **La guía para la asignación de tiempos de auditoría (día-auditor) anexa en este procedimiento.**

3 Evalúa y además coordina con el cliente la necesidad de:

a **Contar con personal de apoyo, tales como expertos técnicos, traductores e intérpretes; para que complementen los conocimientos y habilidades del equipo auditor**

[10] Norma ISO 17021-1, cláusula 9.2.2.- Selección el equipo auditor y asignación de tares.

(experiencia técnica, idioma, manejo de áreas geográficas). En caso de requerirlos éstos actuan bajo la dirección de un auditor, de manera que no influyan indebidamente en la auditoría.

b **Determinar la participación de observadores del equipo auditor, como:**

1º Miembros de ambas partes.
2º Consultores.
3º Personal de acreditación que lleva una testificación, autoridades reglamentarias o cualquier otra persona cuya presencia este justificada.
4º Auditores en formación con la asignación de un auditor como evaluador de éste, el evaluador debe tener la competencia para asumir las tareas y tener la responsabilidad final de las actividades y los hallazgos del auditor en formación.

4 Presenta la información del equipo auditor y demás participantes a la Gerencia General, para su aprobación.

(c) Comunicación al Cliente relativa a los miembros del equipo auditor[11]

1 Cuando se determina la conformación del equipo auditor, el área de SIG informa al cliente y en caso de que éste solicite los antecedentes de los integrantes del equipo, serán otorgados previo cumplimiento de políticas de confidencialidad de la información de ASOCIACIÓN CIVIL BASC PERÚ.

2 El cliente tiene tres (03) días hábiles (de preferencia) para objetar la designación de un auditor o experto técnico en particular, de manera justificada. ASOCIACIÓN CIVIL BASC PERÚ contará con cinco (05) días hábiles para la reconstrucción del equipo auditor conforme a lo establecido en el párrafo 6.-b(2)(b)2e.

(d) Designación de miembros del equipo auditor

El área de SIG confirma la ejecución de la auditoría con cada auditor y hace firmar a los integrantes del equipo auditor determinado, la Declaración de Imparcialidad en mis servicios de auditoría (sin código) para efectos de asegurar la no existencia de conflicto de intereses con la empresa a auditar. Asimismo, entrega al Auditor Líder la información del cliente relativa a su certificación, para que efectúen el diseño del plan de auditoría.

(e) Elaboración del Plan de Auditoría[12]

1 El auditor líder del equipo auditor asignado por ASOCIACIÓN CIVIL BASC PERÚ diseñará un plan para cada etapa de auditoría, en el

[11] Norma ISO 17021-1, cláusula 9.2.3.5.- Comunicación relativa a los miembros de apoyo del equipo auditor.
[12] Norma ISO 17021-1, cláusula 9.2.3.2.- Preparación de plan de auditoría.

formato Plan de Auditoría (F-CISO-012), de acuerdo al programa de auditorías. Este plan de auditoría se basa en requisitos documentados de ASOCIACIÓN CIVIL BASC PERÚ.

2 El líder del equipo auditor, en consulta con el equipo auditor, debe asignar a cada miembro del equipo la responsabilidad de auditar procesos, funciones, sitios, áreas o actividades específicas. Esta asignación debe tener en cuenta la necesidad de competencias, el empleo eficaz y eficiente del equipo auditor, así como los diferentes roles y responsabilidades de los auditores, los auditores en formación y expertos técnicos. Estos últimos, no debe actuar como auditor en el equipo auditor, deberán acompañar siempre al auditor designado en el plan, podrán proporcionar asesoría para la planificación y ejecución de la auditoría.

(f) Comunicación del Plan de Auditoría[13]

1 El auditor líder comunicará el plan de auditoría al área de SIG con un tiempo no mayor o igual a diez (10) días calendario previo a la auditoría, siempre y cuando la empresa haya enviado su documentación con la debida antelación; de no haber correcciones el área de SIG comunicará al cliente el plan de auditoría al día siguiente hábil de recibir el documento por parte del auditor antes de la auditoría "in situ" o "remota". Para ambos casos, **en la medida que se pueda aplicar.**

2 El área de SIG se asegurará que se defina por parte del cliente (auditado) un personal guía para la facilitación de la auditoría[14], a menos que se acuerde de otra manera entre el líder del equipo auditor y el cliente. El equipo auditor se asegurará de que los guías no influyan ni interfieran en el proceso de auditoría ni en los resultados de la auditoría. Las responsabilidades de un personal guía serán:

a **Establecer los contactos y horarios para las entrevistas.**
b **Acordar las visitas a partes específicas del local o de la organización.**
c **Asegurarse de que las reglas concernientes a los procedimientos y protección personal y seguridad del local sean conocidas y respetadas por los miembros del equipo auditor.**
d **Presenciar la auditoría en nombre del Cliente.**
e **Proporcionar aclaraciones o informaciones cuando lo solicite un auditor.**

(g) Comunicación a los Miembros del Equipo Auditor[15]

1 Se debe comunicar el Plan de Auditoría a todo el equipo auditor, debiendo requerirle como tareas que:

[13] Norma ISO 17021-1, cláusula 9.2.3.4.- Comunicación del plan de auditoría.
[14] Norma ISO 17021-1, cláusula 9.2.2.2.3.- Guías.
[15] Norma ISO 17021-1, cláusula 9.2.3.3 Comunicación de tareas al equipo auditor.

a **Examine y verifique la estructura, las políticas, los procesos, los procedimientos, los registros y los documentos relacionados del cliente pertinentes al sistema de gestión.**

b **Determine que éstos cumplen todos los requisitos pertinentes al alcance previsto de la certificación.**

c **Determine que los procesos y procedimientos se han establecido, implementado y mantenido eficazmente para dar confianza en el sistema de gestión del cliente.**

d **Comunique al cliente, para que actúe en consecuencia ante cualquier incoherencia entre su política, sus objetivos y metas (coherentes con las expectativas de la norma aplicable al sistema u otro documento y los resultados).**

2 El equipo auditor también es informado de los riesgos asociados, incluyendo si es necesario algún requisito previo tanto de seguridad como de salud (ejemplo, cursos previos de seguridad, seguros de vida, equipos de protección personal y otros que considere el cliente y ASOCIACIÓN CIVIL BASC PERÚ.

3 Asimismo, se les debe acotar:

a **Toda documentación digital o física que el auditor genere como parte del proceso de auditoría deberá ser resguardada por el auditor y ser considerada confidencial. No deberá ser expuesta y sólo podrá ser entregada a BASC al término de la auditoría. El contenido de los comentarios y apuntes deberá ceñirse sólo a detallar la conformidad y no conformidad del proceso evitando comentarios que puedan criticar y/o juzgar el proceso. El auditor podrá mostrar sus apuntes sólo a la Gerencia General del cliente si éste lo solicita.**

b **Al retirarse de las oficinas, el auditor deberá bloquear su computadora para resguardar la información y en caso de mantener algún medio físico o alguna nota deberá ser responsable de mantenerla de manera segura.**

c **En cada proceso de certificación, renovación, seguimiento u otra visita especial, deberá llenarse el registro de Verificación de Data Cliente (F-CISO-047) para validar la información consignada en la solicitud inicialmente y si esta ha variado de visita en visita.**

c. EJECUCIÓN DE LA CERTIFICACIÓN

(1) Auditoría de Certificación Inicial - Generalidades[16]

(a) AUDITORÍA DE LA ETAPA 1

1 La auditoría de la Etapa 1 debe realizarse con el fin de:

[16] Norma ISO 17021-1, cláusula 9.3.- Certificación Inicial.

a **Auditar la documentación del sistema de gestión del cliente.**

b **Evaluar la ubicación y las condiciones específicas del local del cliente e intercambiar información con el personal del cliente con el fin de determinar el estado de preparación para la auditoría de la Etapa 2.**

c **Revisar el estado del cliente y su grado de comprensión de los requisitos de la norma, en particular en lo que concierne a la identificación de desempeños clave o de aspectos, procesos, objetivos y funcionamientos significativos del sistema de gestión.**

d **Recopilar la información necesaria correspondiente al alcance del sistema de gestión, que incluye:**

1º Las ubicaciones del cliente,
2º Los procesos y equipos empleados,
3º los niveles de controles establecidos (particularmente en caso de clientes multisitio)
4º Los requisitos legales y reglamentarios aplicables; y su cumplimiento (por ejemplo, aspectos de calidad, ambientales, legales del funcionamiento del cliente, los riesgos asociados, etc.). Veáse Anexo H.

e **Revisar la asignación de recursos para la auditoría de la Etapa 2 y acordar con el cliente los detalles de esta.**

f **Proporcionar un enfoque para la planificación de la auditoría de la Etapa 2, obteniendo una comprensión suficiente del sistema de gestión del cliente y de las operaciones del sitio en el contexto de los posibles aspectos significativos.**

g **Evaluar si las auditorías internas y la revisión por la dirección se planifican y realizan, y si el nivel de implementación del sistema de gestión confirma que el cliente está preparado para la auditoría de la Etapa 2.**

h **Asegurar y confirmar los recursos y tiempos para la auditoría con ayuda del Documento Apoyo al Auditor (D-CISO-011).**

i **La auditoría de Etapa 1 deberá indicar la justificación de no auditar un turno de trabajo y la no aplicabilidad de algún requisito.**

2 En la Etapa 1 se evaluará por parte del equipo auditor los siguientes requisitos del Sistema de Gestión:

a **Contexto y alcance del sistema de gestión.**

b **Documentos obligatorios para el sistema de gestión.**
c **Riesgos asociados para el sistema de gestión.**
d **Revisión por la dirección.**
e **Resultados de la última auditoría interna.**
f **En caso de auditorías de Re-Certificación, y si hubiera esta etapa, se efectuará el control del cumplimiento del Reglamento para el uso de Marcas de Certificación ISO (D-CISO-006)[17].**

3 La auditoría de la Etapa 1 se llevará a cabo en las instalaciones del cliente o de manera remota (cuando aplique), para alcanzar los objetivos declarados anteriormente. Para el caso de renovación de la certificación solo se realizará auditoría Etapa 1 en el caso de que se hayan producido cambios significativos en el sistema de gestión, por ejemplo, el cliente o el contexto en el que opera el Sistema de Gestión (por ejemplo, cambios en la legislación).

4 Los hallazgos de la auditoría de la Etapa 1 se documentan directamente al Reporte de Auditoría de la Etapa 1 (F-CISO-016) y se comunican al cliente en la reunión de cierre. Asimismo, se debe informar que el cierre de las acciones pendientes detectadas en la Etapa 1 se efectúa en la auditoría Etapa 2, de no ser tratadas podrían ser clasificadas como No Conformidades.

5 El Reporte de Auditoría de la Etapa 1 (F-CISO-016) es revisado por por el auditor líder dejando el registro de conformidad para liberación de proceso de auditoria etapa 2.

6 Se ha diseñado el Documento de Apoyo Auditor (D-CISO-011), que es una herramienta que permitirá al auditor validar y confirmar la ejecución de actividades en pro del cumplimiento de los objetivos de la auditoría de tercera parte en cada una de sus etapas, conforme a los requisitos de la Norma ISO 17021.

7 Registros soportes Auditoría ETAPA 1
Los registros soportes del cumplimiento de las actividades definidas en este procedimiento para la Etapa 1 son:

a **Plan de auditoría (F-CISO-012)**
b **Programa de Auditoría (F-CISO-013)**
c **Reporte de Auditoría Etapa 1 (F-CISO-016)**
d **Verificación Data Cliente (F-CISO-047)**
e **Lista de Verificación (F-CISO-002) – Opcional**

8 PERU CERTIFICATIÓN a delegado la autoridad en el auditor líder del equipo auditor, para la determinación de la conformidad de la etapa 1 de auditoria y la liberación del proceso de auditoria etapa 2 de certificación. Evidencia de lo anterior es dejada en F-CISO-016 Reporte de auditoria etapa 1,

[17] Norma ISO 17021-1 cláusula 8.3.- Referencia de la certificación y utilización de marcas.

(b) AUDITORÍA DE LA ETAPA 2

1 El propósito de la auditoría de Etapa 2 es evaluar la implementación, incluida la eficacia del sistema de gestión del cliente. La auditoría de Etapa 2 debe tener lugar en las instalaciones del cliente. Debe incluir al menos lo siguiente:

a **La información y las evidencias de la conformidad con todos los requisitos de la norma de sistemas de gestión aplicable u otro documento normativo.**
b **La realización de actividades de seguimiento, medición, reporte y revisión con relación a los objetivos y metas de desempeño clave (coherentes con las expectativas de la norma de sistemas de gestión u otro documento normativo aplicable).**
c **La capacidad del sistema de gestión del cliente y su desempeño en relación con el cumplimiento de requisitos legales, reglamentarios y contractuales aplicables. Véase Anexo H.**
d **Los controles operacionales de los procesos del cliente.**
e **Las auditorías internas y la revisión por la dirección.**
f **La responsabilidad de la dirección en relación con las políticas del cliente.**
g **En caso de tener una no conformidad de la acción pendiente de Etapa 1 efectuar la verificación de la eficacia de las acciones.**
h **En caso de auditorías de seguimiento, se efectuará el control del cumplimiento del Reglamento para el uso de Marcas de Certificación ISO (D-CISO-006).**

2 Registros soportes Auditoría de la ETAPA 2
Los registros soportes del cumplimiento de las actividades definidas en este procedimiento para la Etapa 2 son:

a **Plan de auditoría (F-CISO-012)**
b **Programa de Auditoría (F-CISO-013)**
c **Solicitud de Acción Correctiva (F-CISO-015)**
d **Reporte de auditoría Etapa 2 (F-CISO-017)**
e **Verificación Data Cliente (F-CISO-047)**
f **Lista de verificación (F-CISO-002) - Opcional**

(2) Actividades auditoría “in situ” o “remota” equipo auditor[18]

(a) Reunión de apertura
El auditor líder se encargará de dirigir la reunión de apertura conforme lo establecido en el Documento de Apoyo Auditor (D-CISO-011). Debe ser realizada con la dirección del cliente y cuando sea apropiado, con los responsables de las funciones o procesos que se van a auditar.

[18] Norma ISO 17021-1 cláusula 9.4.- Realización de auditorías.

(b) Comunicación durante la auditoría

1 Durante la auditoría, el equipo auditor debe evaluar periódicamente el progreso de la auditoría e intercambiar información para lo cual definirán en el plan de auditoría unos espacios de tiempo de coordinación con el equipo auditor. El líder del equipo auditor reasignará, si fuera necesario, el trabajo entre los miembros del equipo auditor para asegurar el logro de los objetivos de la auditoría y comunicar periódicamente al cliente el progreso de la auditoría y cualquier inconveniente. En caso se cuente con la participación de un experto técnico, asegurar que este no influya en la auditoría, el experto técnico solo debe proporcionar asesoría técnica y legal al auditor y dirigirse a este directamente, de ser necesario tomar nota y entregar al auditor para su evaluación y calificación.

2 Cuando las evidencias disponibles de la auditoría indiquen que los objetivos de la auditoría no son alcanzables o sugiera la presencia de un riesgo inmediato y significativo (por ejemplo, en materia de seguridad), el líder del equipo auditor debe informar de este hecho al cliente y, si es posible, al organismo de certificación para determinar las acciones apropiadas.

3 Estas acciones pueden incluir la reconfirmación o la modificación del plan de auditoría, cambios en los objetivos de la auditoría o en su alcance, o la finalización de la auditoría. El líder del equipo auditor debe informar a ASOCIACIÓN CIVIL BASC PERÚ del resultado de las acciones tomadas.

4 El líder del equipo auditor debe revisar con el cliente cualquier necesidad de modificación del alcance de la auditoría que surja a medida que avancen las actividades de la auditoría “in situ” o “remota” e informar a ASOCIACIÓN CIVIL BASC PERÚ.

(c) Recopilación y Verificación de la Información

1 Durante la auditoría, la información pertinente para los objetivos, el alcance y los criterios de la auditoría (incluyendo la información relacionada con las interfaces entre funciones, actividades y procesos, así como el control de uso de marca de certificación, si corresponde) se recopilarán mediante un muestreo apropiado, y verificará para convertirse en evidencias de auditoría.

2 Los métodos utilizados por el equipo auditor para recopilar la información incluyen, entre otros:

a **Las entrevistas.**
b **La observación de los procesos y las actividades; y**
c **La revisión de la documentación y de los registros.**

(d) Identificación y Registro de los Hallazgos de Auditoría

1 Los hallazgos de auditoría que resumen la conformidad y detallan las No Conformidades, así como las Evidencias de Auditoría que las respaldan, se registran en el Reporte de Auditoría directamente.

2 Los tipos de Hallazgos para ASOCIACIÓN CIVIL BASC PERÚ, posibles en un proceso de auditoría de Certificación en su orden de criticidad en cualquiera de sus partes son:

a **No Conformidad Mayor: No conformidad que afecta a la capacidad del sistema de gestión para lograr los resultados previstos.**
Las no conformidades pueden ser clasificadas como mayores en las siguientes circunstancias:
1º si existe una duda significativa de que se haya implementado un control eficaz de proceso, o de que los productos o servicios cumplan los requisitos especificados;
2º una cantidad de no conformidades menores asociadas al mismo requisito o cuestión podría demostrar una desviación sistemática y, por tanto, constituye una no conformidad mayor.

b **No Conformidad Menor: No conformidad que no afecta la capacidad del sistema de gestión para lograr los resultados previstos. Ejemplo: Incumplimiento parcial de un requisito o cuando se incumpla el Reglamento para el uso de Marcas de Certificación ISO (D-CISO-006).**

c **Oportunidad de Mejora: Actividad para mejorar el desempeño.**

d **Fortaleza: Se excede en el cumplimiento del requisito.**

3 Un hallazgo de No Conformidad se registrará con relación a un requisito específico de los criterios de auditoría, debe contener una mención clara de la No Conformidad e identificará en detalle las evidencias objetivas en las que se basa la No Conformidad. Se registran en el formato Solicitud de Acción Correctiva (F-CISO-015).

4 El líder del equipo auditor debe intentar resolver todas las diferencias de opinión sobre las evidencias o los hallazgos de la auditoría, entre el equipo auditor y el cliente. Se deben registrar los puntos no resueltos.

(e) Preparación de las Conclusiones de Auditoría

En un espacio planeado en el plan de auditoría previo a la reunión de cierre, el equipo auditor:

1 Revisará los hallazgos de auditoría y cualquier otra información apropiada reunida durante la auditoría, con respecto a los objetivos y los criterios de la auditoría, y clasificar las no conformidades.

2 Acordará las conclusiones de la auditoría, teniendo en cuenta la incertidumbre inherente al proceso de auditoría.
3 Identificará toda acción de seguimiento necesaria; y
4 Confirmará que el programa de auditoría es adecuado o identificará cualquier modificación que sea necesaria.

(f) Realización de la Reunión de Cierre

1 El auditor líder se encargará de dirigir la reunión de cierre conforme a lo establecido en el Documento de Apoyo Auditor (D-CISO-011). Debe ser realizada con la dirección del cliente y cuando sea apropiado, con los responsables de las funciones o procesos auditados. Se debe registrar la asistencia a esta reunión.

2 Las No Conformidades se comunicarán al Cliente, con el fin de asegurar que las evidencias son exactas, que se entienden y se debe acordar el plazo de respuesta en el registro Solicitud de Acción Correctiva (F-CISO-015); evidencia de lo anterior serán las firmas de las partes de auditoría en señal de consenso, registradas en dicho documento.

3 Asimismo, comunicará al cliente lo siguiente:

a **Deberá enviar su plan de acción a través del registro Solicitud de Acción Correctiva (F-CISO-015), de acuerdo a los plazos establecidos, el cual deberá ser revisado y aceptado por el auditor líder. El proceso de cierre será con la evidencia documentaria de la No Conformidad para el caso de las menores y su efectividad in situ en la próxima visita y en caso de No Conformidades mayores será cerrada in situ, en un plazo no mayor de seis (06) meses.**

b **De no cerrarse una no conformidad menor, ésta genera una no conformidad mayor.**

c **De no cerrarse una no conformidad mayor, en:**
Una auditoría de certificación en etapa 2) se impide el otorgamiento de la certificación, si no puede se puede verificar la implementación de las correcciones y acciones correctivas de cualquier no conformidad mayor dentro de los 6 meses posteriores al último día de la etapa 2, se debe realizar otra auditoría de etapa 2 antes de recomendar la certificación;
En una visita de mantenimiento (auditoría de seguimiento) se solicitará la suspensión del certificado hasta cerrar la no conformidad mayor dentro del año de su visita. De no lograr el cierre efectivo de la no conformidad mayor pese a la suspensión se procederá con el retiro del certificado. De optar por continuar con su Sistema certificado, éste iniciará en Etapa 1.
En una auditoría de Renovación, para recomendar la renovación las correcciones y acciones correctivas se deben de implementar y verificar antes de la experación del certificado.

Caso contrario, si no se puede verificar la implementación de las correcciones y acciones correctivas para cualquier no conformidad mayor antes d ela fecha de expiración del certificado, entonces no se debe de recomendar la renovación y la Asociación Civil BASC PERU podrá restaurar la certificación dentro de los seis (06) meses siguientes, siempre y cuando se hayan completado las actividades de renovación pendientes, de otro modo se de realiza una nueva etapa 2. La fecha de vigencia debe ser la fecha en que se tomó la decisión de la nueva certificación o una posterior, y la fecha de expiración debe basarse en el ciclo de certificación anterior.

d **El equipo auditor no podrá sugerir la causa de las No Conformidades o su solución.**

e **Las diferencias de opinión acerca de los Hallazgos o las Conclusiones de la auditoría entre el Equipo Auditor y el Cliente se discutirán y en la medida de lo posible, resolverse. Las diferencias de opinión que no se resuelvan se registrarán y remitirán en el Formato de Reporte Final según corresponda en el campo Observaciones, a ASOCIACIÓN CIVIL BASC PERÚ, por parte del auditor líder.**

(g) Reporte de Auditoría

1 ASOCIACIÓN CIVIL BASC PERÚ debe proporcionar un reporte escrito de cada auditoría. ASOCIACIÓN CIVIL BASC PERÚ mantiene la propiedad sobre el reporte de auditoría.

2 El líder de equipo auditor es responsable de preparar el reporte de auditoría y de su contenido. El reporte de auditoría se desarrollará conforme los formatos Reporte de Auditoría Etapa 1 (F-CISO-016) y el Reporte de Auditoría Etapa 2/Seguimiento/Renovación (F-CISO-017).

3 En caso de que el auditor líder entregue un informe preliminar al final de la auditoría, éste deberá llevar un sello de agua que indique “PRELIMINAR”.

4 El auditor líder debe informar al final de la auditoría la(s) no conformidad(es) en el formato Solicitud de Acción Correctiva (F-CISO-015), en caso el cliente lo exija.

5 Luego de remitir los Reportes de Auditoría a la ASOCIACIÓN CIVIL BASC PERU, al menos un miembro del Comité de Certificación deberá revisar dichos reportes y evaluar si están correctamente llenados. De encontrar errores como clasificación del hallazgo, identificación de requisitos, redacción de hallazgos, entre otros, el área de SIG envía el reporte de auditoría, vía correo electrónico, al auditor líder para las correcciones pertinentes. El auditor tendrá cuarenta y ocho (48) horas para dar respuesta y envío al reporte final en la medida que sea posible.

6 El reporte de auditoría final será enviado por el área del SIG al cliente, junto con el(los) formato(s) Solicitud de Acción Correctiva (F-CISO-015), **en la medida de lo posible** el reporte de auditoría final (de Etapa 2 por certificación o renovación, seguimiento 1 o 2), se enviará al cliente dentro de los 30 (treinta) días calendario posterior al último día de ejecución de la auditoría.

(h) ANÁLISIS DE LAS CAUSAS DE LAS NO CONFORMIDADES

ASOCIACIÓN CIVIL BASC PERÚ requerirá al cliente de auditoría a través de su equipo auditor, el análisis de las causas y que describa las correcciones específicas y las acciones correctivas realizadas o planificadas, para eliminar las No Conformidades detectadas en el formato Solicitud de Acción Correctiva (F-CISO-015) en los siguientes plazos:

1 Para las acciones pendientes, como resultado de la auditoría Etapa 1, el plazo límite será la fecha de auditoría Etapa 2 coordinada entre el auditor líder y la empresa y;

2 Para las No Conformidades de auditoría Etapa 2: según sea el caso:

a **Mayor, entrega de evidencia de la corrección, así como el análisis de causa y acciones correctivas máximo a los 30 días calendario posterior a la fecha de recepción del informe de auditoría. La verificación de la eficacia de las acciones correctivas se realizará mediante una auditoría adicional, máximo a los 180 días calendario posterior al último día de la etapa 2.**

b **Menor, entrega de evidencia de la corrección, así como el análisis de causa y acciones correctivas (cuando aplique) a las 30 días calendario y máximo a los 60 días calendario posterior a la fecha de recepción del informe de auditoría. La eficacia de las correcciones y/o acciones correctivas se revisarán en una futura auditoría (evidencia documental).**

(i) VERIFICACION DE LA EFICACIA DE LAS CORRECCIONES Y ACCIONES CORRECTIVAS

1 ASOCIACIÓN CIVIL BASC PERÚ a través del líder del equipo auditor revisará las correcciones, el análisis de las causas y las acciones correctivas enviadas por el cliente para determinar si son aceptables.

2 Recibida(s) y revisada(s) la(s) Solicitud(es) de Acción Correctiva (F-CISO-015) el auditor líder deberá informar por escrito al área de SIG la conformidad y aceptación de las mismas, si las considera suficientes y eficaces. El área de SIG, comunicará el resultado la conformidad y aceptación.

3 Si el auditor líder, considera no suficientes y no eficaces las correcciones y acciones propuestas, se repetirá ciclos de revisión y

aprobación por parte del auditor líder durante el tiempo establecido y según clasificación de la no conformidad.

4 El auditor líder determinará si la verificación de la eficacia de la corrección y de la acción correctiva puede realizarse sobre la base de una revisión de la documentación proporcionada por el cliente, o por una verificación “in situ” o “remota”, en este caso deberá informar al área de SIG de ASOCIACIÓN CIVIL BASC PERÚ para coordinar la logística y costos de la nueva visita al cliente de auditoría (Si aplica).

5 De no poder cerrar la(s) No conformidad(es) mayor(es) en la visita de Cierre de No Conformidad, el certificado quedará suspendido y podrá gestionarse una nueva visita de Cierre de No Conformidad Mayor dentro del año de la visita de mantenimiento y en caso de certificación se inicia el proceso como Etapa 1. En caso el cliente no pueda levantar las No conformidades mayores en esta segunda auditoría de cierre el certificado quedará cancelado.

6 Para el caso de una no conformidad en el uso de la marca de certificación ISO, se debe informar al Área de Comunicaciones para que proceda inmediatamente al seguimiento y las comunicaciones a los clientes de acuerdo al procedimiento Comunicaciones con el Asociado y no Asociado (P-COM-001).

(3) Auditorías adicionales

ASOCIACIÓN CIVIL BASC PERÚ informará a la organización auditada si será necesario realizar una auditoría completa adicional, una auditoría parcial adicional o enviar evidencias documentadas (a confirmar durante las auditorías de seguimiento), para verificar la eficacia de las correcciones y de las acciones correctivas. El reporte a utilizar será el Reporte de la Etapa 2, cuando sea el caso.

d. DECISIÓN DE CERTIFICACIÓN[19]

(1) Información para el otorgamiento de la certificación

La información proporcionada por el auditor líder al Comité de Certificación de ASOCIACIÓN CIVIL BASC PERÚ, para permitir que tome una decisión sobre la Certificación, Ampliación o Reducción de alcance, o Re-Certificación, debe incluir como mínimo:

a **Los reportes de auditoría.**
b **Los comentarios sobre las No Conformidades y cuando corresponda, las correcciones, evidencias de las correcciones y acciones correctivas llevadas a cabo por el cliente.**

[19] Norma ISO 17021-1 cláusula 9.5.- Decisión de certificación
Norma ISO 27006 cláusula 9.5.- Decisión de certificación

c **La confirmación de la información proporcionada al organismo de certificación y utilizada para la revisión de la solicitud.**
d **La recomendación de otorgar o no la certificación, junto con cualquier condición u observación.**
e **Registro de Verificación de Data Cliente (F-CISO-047).**
f **Registro Programa de Auditoría (F-CISO-013).**

(2) Revisión de Información

El Comité de Certificación de ASOCIACIÓN CIVIL BASC PERÚ, integrado por personas diferentes a aquellas que llevaron a cabo las auditorías de las Etapas 1 y 2 toma la decisión de otorgar, negar, mantener, ampliar o reducir el alcance, renovar, suspender, restaurar o retirar la certificación soportado en:

(a) La información proporcionada por el equipo auditor validando que sea suficiente con respecto a los requisitos de certificación y al alcance de la certificación.
(b) La revisión, aceptación y verificación de la eficacia de las correcciones y de las acciones correctivas, para todas las No Conformidades que representan.
(c) La revisión y aceptación del plan de correcciones y acciones correctivas del cliente para cualquier otra No Conformidad.
(d) Revisión del registro Verificación de Data Cliente (F-CISO-047) donde se indica si ha habido alguna modificación de lo que declaró el cliente durante la visita y cómo ésta podría variar en el tiempo y si dichas variaciones que puedan afectar la efectividad del proceso han sido declaradas a BASC PERU antes de ejecutarse las visitas.
(e) Como resultado de esta revisión puede considerarse cambios que afecten el proceso de auditoría como: invalidar la auditoría, aumentar los días de auditoría o disminuirlo, cambios en la clasificación de hallazgos, entre otros.
(f) Esta decisión queda sentada en el Acta de Comité - Certificación (F-CISO-037).
(g) Se otorgará la certificación y se procederá a la emisión del certificado acorde a lo establecido.

Para el caso de certificación de SGSST ISO 45001:2018 de aplicar se analizará por parte del comité de certificación la auditoria e inclusión de sitios temporales en el desarrollo de actividades, productos y servicios dentro del control o influencia de la organización que puede afectar el desempeño de la SST de la organización. De contarse con sitios temporales en el alcance de certificación del SGSST ISO 45001:2018 se asegurará que los mismos se registren dentro del contenido de la certificación expedida al cliente de auditoria por parte de PERU CERTIFICATION.

e. MANTENIMIENTO DE LA CERTIFICACIÓN[20]

(1) ASOCIACIÓN CIVIL BASC PERÚ mantendrá la certificación basándose en la demostración de que el cliente de auditoría continúa cumpliendo los requisitos de la Norma.

[20] Norma ISO 17021-1 cláusula 9.6.- Mantenimiento de la certificación.

(2) Puede mantener la certificación de un cliente sobre la base de una conclusión favorable formulada por el líder del equipo auditor, sin tener que proceder a una revisión independiente posterior, a condición de que:

(a) Para cualquier No Conformidad mayor u otra situación que puede llevar a suspender o retirar la certificación, el líder del equipo auditor reporte a ASOCIACIÓN CIVIL BASC PERÚ sobre la necesidad de iniciar una revisión por personal competente adecuado y diferente de aquel que ha llevado a cabo la auditoría, con el fin de determinar si se puede mantener la certificación. El auditor líder podrá reportarlos al Comité de Certificación.

(b) El personal competente de ASOCIACIÓN CIVIL BASC PERÚ debe realizar un seguimiento de sus actividades de seguimiento, incluido el seguimiento de los reportes de sus auditores, con el fin de confirmar que la actividad de certificación funciona de manera eficaz.

(3) Actividades de Vigilancia a la Certificación

(a) ASOCIACIÓN CIVIL BASC PERÚ realizará actividades de vigilancia de manera que se realice el seguimiento regular de las áreas y funciones representativas, cubiertas por el alcance del Sistema de Gestión certificado, y se tengan en cuenta los cambios en el cliente certificado y en su sistema de gestión.

(b) Las actividades de vigilancia incluyen auditorías de control in “situ” o “remota”, que evalúan el cumplimiento del Sistema de Gestión. La viabilidad de las auditorías de control y responsabilidad de atenderlas se establecen en el acuerdo de certificación firmado por el cliente de auditoría y BASC PERÚ.

(c) Las visitas de vigilancia son llevadas a cabo como resultado de las auditorías o de alguna información o acción que afecte a la efectividad del sistema de gestión.

(d) Otras actividades de vigilancia realizada por parte de ASOCIACIÓN CIVIL BASC PERÚ incluyen:

1 La petición de información del organismo de certificación al cliente certificado sobre aspectos relativos a la certificación.
2 La revisión de cualquier declaración del cliente relativa a sus operaciones (por ejemplo, material promocional, sitios en internet, etc.)
3 La solicitud al cliente para que proporcione documentos y registros (en papel o en soporte electrónico), y
4 Otros medios de seguimiento del desempeño del cliente certificado.

(4) Auditoría de Seguimiento

(a) Las auditorías de seguimiento son auditorías “in situ” o “remota”, pero no son necesariamente auditorías de todo el sistema y se planifican en el

programa de auditoría elaborado por el líder del equipo auditor y aprobado por el área de SIG, de manera que se pueda confiar en que el sistema de gestión certificado continúa cumpliendo los requisitos entre las auditorías de renovación de la certificación. El plan de auditoría para auditorías de seguimiento por parte de ASOCIACIÓN CIVIL BASC PERÚ debe incluir pero no limitarse a la revisión por parte del equipo auditor de:

1 Las auditorías internas y revisión por la dirección.
2 La revisión de las acciones tomadas sobre las No Conformidades identificadas durante la auditoría previa.
3 El tratamiento de las quejas.
4 La eficacia del sistema de gestión en relación con el logro de los objetivos del cliente certificado.
5 El progreso de las actividades planificadas dirigidas a la mejora continua.
6 La continuidad en el control operativo.
7 La revisión de cualquier cambio.
8 La utilización de marcas y/o cualquier otra referencia a la certificación.
9 Eficacia de no conformidades emitidas en la visita anterior.

Las auditorías de seguimiento deben realizarse al menos una vez al año. La fecha de la primera auditoría de seguimiento después de la certificación inicial no debe realizarse transcurridos más de doce (12) meses desde la fecha en que se tomó la decisión sobre la certificación, no se podrá extender dicho plazo, salvo razones de fuerza mayor. Para las siguientes auditorías de seguimiento, no necesariamente se programarán cada doce (12) meses, puede ser necesario ajustar la frecuencia de las auditorías de seguimiento para adaptarse a factores como las estaciones del año o la certificación de sistemas de gestión de duración limitada, entre otros, esto deberá estar debidamente justificado; por lo cual, podrán programarse dos (02) meses después de cada vencimiento anual; en el caso se desee ampliar dicho plazo, este no deberá exceder los seis (06) meses después de cada vencimiento anual, los cuales se concederán previa aprobación del Comité de Certificaciones ISO.

(b) Se ejecutan de acuerdo a lo establecido en el párrafo 6.-c(2) Actividades auditoría “in situ” o “remota” equipo auditor.

(c) Los resultados de las auditorías de seguimiento se plasmarán en el formato de Reporte de auditoría Etapa 2 (F-CISO-017) y si corresponde, se continuará con las actividades descritas en el párrafo 6.-c(2)(h)ANÁLISIS DE LAS CAUSAS DE LAS NO CONFORMIDADES y VERIFICACION DE LA EFICACIA DE LAS CORRECCIONES Y ACCIONES CORRECTIVAS

(5) Renovaciones

(a) Las renovaciones serán llevadas a cabo como una auditoría inicial, sin embargo, sólo a aquellas empresas que no hayan producido cambios significativos en el sistema de gestión, no será necesario una auditoría de

Etapa 1 sino directamente se llevará a cabo la Etapa 2 para confirmar la continuidad y efectividad del Sistema.

(b) Para aquellas empresas que durante su periodo de vigencia de su certificado sea necesario que las actividades de la auditoría de renovación incluyan una etapa 1, en situaciones en las que se hayan producido cambios significativos en el sistema de gestión, la organización o el contexto en el que opera el sistema de gestión (por ejemplo, cambios en la legislación).

(c) En caso de no demostrar efectividad de cierre se generará una No Conformidad mayor o menor según la criticidad del hallazgo.

(d) Cabe resaltar que las renovaciones se tienen que llevar a cabo dentro del mes antes que termine la vigencia del certificado de lo contrario se contará como auditoría inicial, el cual el cliente podrá restaurar su certificación hasta 180 días después.

(e) El plan del proceso de renovación considerará en sus tiempos la revisión de los reportes de auditorías anteriores y el cierre efectivo de las no conformidades menores de la auditoría anterior. De no existir el cierre efectivo de la no conformidad menor se procederá a generar una no conformidad mayor.

(f) La auditoría de Etapa 2 se llevará a todos los procesos de la empresa y se tendrá en consideración:

1 La eficacia del Sistema y su aplicabilidad en su alcance
2 El compromiso de mejora continua
3 Logro de la Política y sus objetivos
4 Apelaciones y quejas de certificaciones

(g) Se considera una renovación cuando se está concluyendo el periodo de 03 (tres) años de la certificación, sin embargo, cuando una no conformidad mayor no ha sido cerrada antes del vencimiento del certificado, se deberá llevar a cabo la Etapa 1 y Etapa 2, como nuevo proceso de certificación.

(6) Auditorías especiales

(a) AMPLIACIÓN DEL ALCANCE

1 Cuando una organización desea ampliar el alcance de la certificación como incrementar los locales o los procesos certificados lo hacen a través del formato Solicitud de Certificación - Renovación (F-CISO-001) y lo envía a ASOCIACIÓN CIVIL BASC PERÚ.

2 Se conformará el equipo auditor según lo previsto en el Procedimiento de Selección, Determinación y Evaluación de Competencias del Equipo Auditor, quienes revisan que esté cumpliendo satisfactoriamente con lo estipulado en los procedimientos de seguimiento de la certificación, que haya desarrollado

satisfactoriamente la totalidad de las Auditorías de seguimiento programadas hasta la fecha en la cual la ampliación de la certificación, y esté cumpliendo con las políticas y compromisos acordados.

3 Se realiza las actividades de auditoría necesarias para decidir si se concede o no la ampliación de la certificación, esto incluye las actividades de la Etapa 1 y 2 y la decisión de certificación como figura en este procedimiento.

4 Las auditorías para ampliar el alcance de la certificación pueden realizarse en el momento de una auditoría en conjunto con las auditorías de seguimiento, según las necesidades del cliente.

5 La ampliación del alcance puede influir un aumento de tiempos de auditoría, esto dependerá de la cantidad de empleados que la ampliación incluya.

(b) AUDITORÍAS CON NOTIFICACIÓN A CORTO PLAZO O DE CIERRE

1 ASOCIACIÓN CIVIL BASC PERÚ podrá realizar auditorías a clientes bajo la forma de visitas notificadas a corto plazo con el fin de investigar quejas, en respuesta a cambios o como seguimiento de clientes con la certificación suspendida. En estos casos:

a **Se describirá y pondrá en conocimiento de los clientes certificados con antelación las condiciones en las que se van a efectuar estas visitas con notificación a corto plazo, y**

b **Se pondrá un cuidado muy especial en la designación del equipo auditor debido a la imposibilidad por parte de la organización auditada de formular una objeción sobre los miembros del equipo auditor.**

2 Dentro de este tipo de auditorías se encuentran las auditorías de cierre de No Conformidad Mayor ejecutadas por parte de ASOCIACIÓN CIVIL BASC PERÚ.

3 Para esta auditoría de Cierre de No Conformidad Mayor se llevará el proceso de Etapa 2 y de generarse alguna no Conformidad menor se procederá a tomar en cuenta los plazos establecidos para cierre de no conformidad menor en Etapa 2. De no poder cerrar la(s) No conformidad(es) mayor(es) en la visita de Cierre de No Conformidad, el certificado quedará suspendido y podrá gestionarse una nueva visita de Cierre de No Conformidad Mayor dentro de los próximos dos (02) meses. En caso el cliente no pueda levantar las No conformidades mayores en esta segunda auditoría de cierre el certificado quedará cancelado.

4 Asimismo, si hay una administración inapropiada del sistema de Gestión o alguna queja a la compañía que pueda afectar la efectividad del Sistema de Gestión, Asociación Civil BASC PERÚ tiene la autoridad de llevar a cabo una auditoría inopinada.

5 Investigación de Accidentes graves o muertes dentro del SGSST ISO 45001:2018.

6 A.1.6 MD 22:2019 Si las instalaciones y áreas de trabajo del cliente de auditoria están sujetas a cierre, PERU CERTIFICATION verificará que el SGSTT sigue cumpliendo con ISO 45001:2018 y que se implementa de manera efectiva con respecto a las instalaciones cerradas y áreas de trabajo y, en caso contrario, suspender el certificado.

(7) Suspender, retirar o reducir el alcance de la certificación

(a) En el formato Acuerdo de Certificación (F-CISO-006) establecido entre BASC PERÚ y el Cliente de auditoría, se establecen las causales para suspender, retirar o reducir el alcance de la certificación, entre las que están:

1. El sistema de gestión certificado del cliente ha dejado de cumplir de forma persistente o grave los requisitos de la certificación, incluidos los requisitos relativos a la eficacia del sistema de gestión;
2. El cliente certificado no permite la realización de las auditorías de seguimiento o de renovación de la certificación de acuerdo con la periodicidad requerida;
3. La organización certificada ha pedido voluntariamente una suspensión; y
4. No se cumpla con los pagos pactados en el proceso de certificación, excepto cuando exista un compromiso de pago vigente.
5. Si en el periodo de la certificación (seguimiento 1 y/o seguimiento 2) no se evidencia la realización de una o más de una de las actividades identificadas en el alcance de certificación, la empresa deberá demostrarlo previo a la solicitud de la renovación, de lo contrario se reducirá/modificará el alcance.

(b) Una vez una certificación sea suspendida o retirada a un cliente éste debe dejar de usar toda publicidad que contenga alguna referencia a una condición de certificado y BASC PERÚ lo eliminará de su Base de Datos de clientes certificados mantenida en su web. Para los casos en que se presente la reducción de alcance se realizarán las modificaciones respectivas en el alcance en la Base de Datos de clientes certificados.

(c) Cuando no se resuelvan los problemas que dieron lugar a la suspensión en el plazo establecido por BASC PERÚ, se debe retirar o reducir el alcance de certificación.

(d) La suspensión de una certificación a un cliente no debe superar los seis (06) meses.

(e) Se debe informar al Área de Comunicaciones para que proceda inmediatamente al seguimiento de uso de marcas y las comunicaciones a los clientes de acuerdo al procedimiento Comunicaciones con el Asociado y no Asociado (P-COM-001).

(f) A.1.5 MD 22:2019 El incumplimiento legal deliberado o constante se considerará una falla grave para respaldar el compromiso de la política para

lograr el cumplimiento legal y excluirá la certificación o hará que un certificado estándar del SGSTT ISO 45001 se suspenda o retire.

f. APELACIONES[21]

ASOCIACIÓN CIVIL BASC PERÚ cuenta con un procedimiento documentado de Gestión de Apelaciones (P-CISO-002), para recibir, evaluar y tomar decisiones relativas a las apelaciones que se presenten por conceptos negativos de certificación.

g. QUEJAS[22]

ASOCIACIÓN CIVIL BASC PERÚ cuenta con un procedimiento documentado de Quejas y Sugerencias (P-COM-003) para dar tratamiento a las quejas que se pudieran presentar por los clientes de certificación sobre el proceso.

h. REGISTROS RELATIVOS A SOLICITANTES Y CLIENTES[23]

(1) ASOCIACIÓN CIVIL BASC PERÚ mantiene los registros relativos a la actividad de auditoría y certificación de todos los clientes, incluidas todas las organizaciones que presentaron solicitudes, así como todas las organizaciones auditadas, certificadas o a las que se le suspendió o retiró la certificación.

(2) Los registros, relativos a los clientes certificados, que se conservan son los siguientes:

(a) La información relativa a la solicitud y los reportes de auditoría inicial, de seguimiento y de renovación de la certificación.
(b) El acuerdo de certificación
(c) La justificación de la metodología utilizada para el muestreo de sitios, según sea apropiado; NOTA: La metodología de muestreo incluye el muestreo utilizado para evaluar el sistema de gestión específico y/o para seleccionar los locales en el contexto de una evaluación multi locales.
(d) La justificación para la determinación del tiempo asignado al equipo auditor/auditores (véase el apartado 9.1.4 de la Norma ISO 17021-1)
(e) La verificación de las correcciones y acciones correctivas
(f) Los registros de las quejas y apelaciones, y cualquier corrección o acción correctiva subsiguiente
(g) Las deliberaciones y decisiones del Comité, cuando corresponda
(h) La documentación relativa a las decisiones de certificación
(i) Los documentos de certificación, incluido el alcance de la certificación con respecto al producto, proceso o servicio, según sea el caso.
(j) Los registros relacionados que son necesarios para establecer la credibilidad de la certificación, tales como evidencia de la competencia de los auditores y expertos técnicos

[21] Norma ISO 17021-1 cláusula 9.7 Apelaciones.
[22] Norma ISO 17021-1 cláusula 9.8 Quejas.
[23] Norma ISO 17021-1 cláusula 9.9 Registros relativos a los clientes.

(3) ASOCIACIÓN CIVIL BASC PERÚ conserva los registros relativos a los solicitantes y clientes de forma segura, con el fin de asegurar que la información se mantenga confidencial. Los registros se transportan, transmiten o transfieren de forma que se asegure el mantenimiento de la confidencialidad.

(4) Para aplicar control sobre los registros relativos a los solicitantes y clientes, ASOCIACIÓN CIVIL BASC PERÚ aplica el procedimiento Control de Documentos y Registros, en el que se establece el manejo de listas maestras de documentos y de registros, este último establece el tiempo de retención de los registros durante el tiempo que dure el ciclo en curso, más un ciclo completo de certificación.

(5) La ampliación de este punto en lo que respecta al manejo documentario y de información hacia los clientes se detalla a través del procedimiento Gestión de las Comunicaciones (P-CISO-009).[24]

i. ACTUALIZACIÓN DE INFORMACIÓN DE LOS CLIENTES

(1) La actualización de la información de los clientes tales como alcance, dirección, tamaño de la organización, cambios que puedan afectar al Sistema de Gestión, así como los de acción fiscal como representantes de la organización etc., deberán ser informados a ASOCIACIÓN CIVIL BASC PERÚ por parte del cliente antes de su proceso de auditoría. Así mismo, se confirmará con el cliente a través del envío del plan de auditoría si la información que consigna BASC PERÚ ha cambiado o se mantiene vigente.

(2) Sin embargo, en cada auditoría al Sistema de Gestión, se validará información referente al Sistema como el alcance, tamaño de la organización, responsables del Sistema. En caso de existir diferencias que puedan afectar el proceso de auditoría como es ampliación y/o reducción de alcance o incremento o disminución de personal que está incluido en el alcance, se realizará la comunicación inmediatamente a las oficinas para que un ejecutivo se comunique con la organización y se proceda a regularizar la información y el proceso de certificación.

j. TRANSICION DE NORMAS

[24] Norma ISO 17021-1 cláusula 8.1 Información Pública.

(1) Cuando una norma cambie de versión, la organización tiene el plazo que determine la organización ISO para culminar la implementación, adecuarse a la nueva Norma (en algunos casos es 03 años) y llevar a cabo la transición a la nueva versión. Esto no impide que cualquier empresa pueda certificar en la versión anterior de la norma.

(2) Para el proceso de transición se deberá tener en cuenta lo siguiente:

(a) Comunicación a los clientes del periodo máximo de vigencia de su certificado de certificación actual.
(b) Comunicar el proceso de transición de la norma.
(c) Establecer los tiempos de auditoría para la transición a la nueva versión.
(d) Ejecutar la auditoría de transición.
(e) Emitir el nuevo certificado vigente, previa solicitud del certificado anterior.

(3) Proceso de Transición

(a) La Transición debe llevarse a cabo antes de que el certificado anterior entre fuera de vigencia y el tiempo que se establece es de (01) un mes, tiempo establecido para la emisión del certificado y entrega del mismo al cliente, así el Sistema se mantiene vigente de manera continua.

(b) La transición puede llevarse a cabo durante las visitas programadas al cliente ya sea en una certificación nueva, renovación o visita de seguimiento y los tiempos establecidos incluyen el proceso de transición.

(c) Si el cliente considera una visita adicional de transición a la nueva norma los tiempos establecidos son considerados como una visita de seguimiento de acuerdo a los días auditor que se obtuvieron de su respectivo programa de auditoría (1/3 de días auditor obtenido de la visita de certificación).

(d) La visita se realiza como cualquier proceso de auditoría Etapa 2. Los registros son los utilizados en auditorías de Etapa 2.

(e) Las no conformidades ya sean mayores y/o menores resultantes de la visita tienen tratamiento como Etapa 2.

(f) En caso de no llevar a cabo la transición o de no llevar a cabo un cierre efectivo de una no conformidad mayor, se deberá solicitar al cliente el certificado anterior, al día siguiente de no estar vigente dicho certificado. Y se contaría como nuevo proceso de certificación en caso el cliente decida seguir con su proceso.

Para transiciones de certificación ISO/IEC 27001 se dará cumplimiento a IAF MD 26:2022

- PERU CERTIFICATION puede realizar la auditoría de transición junto con la auditoría de seguimiento, la auditoría de recertificación o mediante una auditoría separada.
- La auditoría de transición no se basará únicamente en la revisión de documentos, especialmente para la revisión de los controles tecnológicos.
- La auditoría de transición deberá incluir, entre otros, lo siguiente:
  a. el análisis de brechas de ISO/IEC 27001:2022, así como la necesidad de cambios en el SGSI del cliente;
  b. la actualización de la declaración de aplicabilidad (SoA);
  c. En su caso, la actualización del plan de tratamiento de riesgos.

Como mínimo, la auditoría de transición debe incluir 0,5 días de auditor adicionales para confirmar la transición de los clientes certificados cuando la transición se realice durante una auditoría de vigilancia o como auditoria separada.

PERU CERTIFICATION puede definir el cronograma para la presentación de la solicitud de transición por parte de los clientes certificados en el programa de auditoría de transición;

PERU CERTIFICATION tomará la decisión de transición con base en el resultado de la auditoría de transición;

PERU CERTIFICATION debe actualizar los documentos de certificación para el cliente certificado si su SGSI cumple con los requisitos de ISO/IEC 27001 en su versión vigente.

Nota: Cuando el documento de certificación se actualice porque el cliente completó con éxito solo la auditoría de transición, no se cambiará el vencimiento de su ciclo de certificación actual.

4) Todas las certificaciones basadas en ISO/IEC 27001:2013 vencerán o se retirarán al final del período de transición.

k. EMISION DE CERTIFICADO[25]

(1) Una vez que se decide otorgar la certificación, el área de SIG se encargará de entregar al Cliente:

(a) El certificado físico / digital.
(b) El documento “Reglamento para el Uso de las Marcas de Certificación ISO” (D-CISO-006).

(2) El certificado tendrá como fecha de emisión, el día en que el Comité de Certificación toma la decisión de certificación.

[25] Norma ISO 17021-1 cláusula 8.2.- Documentos de certificación

(3) Para el caso de transferencias de certificaciones, el certificado tendrá como fecha de emisión un día después de entrar fuera de vigencia el certificado anterior, cuya nueva vigencia será de 3 años. En caso, la vigencia anterior sea posterior a la toma de decisión, se mantendrá lo indicado en el punto anterior.

(4) El certificado deberá contener la siguiente información obligatoria:

(a) Nombre del cliente certificado
(b) Ubicación geográfica del o los sitios certificados
(c) Fecha efectiva de otorgamiento, será la misma de la toma de decisión del Comité de Certificación, considerada como la fecha de inicio del periodo de certificación.
(d) Fecha de expiración del certificado: tres años desde la fecha de inicio, siempre y cuando los resultados de las auditorías de seguimiento hayan sido favorables o el ciclo de certificación no se vea interrumpido por otros aspectos declarados en el presente procedimiento.
(e) Fecha de Revisión del certificado, puede darse por cualquier cambio en las condiciones de certificación inicial (ampliación/reducción del alcance; cambio de domicilio; levantamiento de suspensión, etc.)
(f) Fecha de expiración del último ciclo de certificación (cuando aplique)
(g) Fecha de auditoría de renovación
(h) Código único de identificación del cliente certificado
(i) Norma de Sistema de Gestión empleada para la auditoría del cliente certificado
(j) Alcance de la certificación, según sea el caso, y por cada sitio certificado.
(k) Nombre y Marca del Organismo de Certificación, pudiendo emplear la Marca del ente acreditador, según el reglamento de Uso de Marcas.
(l) Declaración de Aplicabilidad (aplica para ISO/IEC 27001), conforme a lo declarado en el reporte de auditoría, en caso la organización realice cambios en la SoA que afectan a la cobertura de los controles, se emitirá un nuevo certificado.

(5) Para el caso de Procesos de Transición, para la entrega del certificado nuevo se deberá de consignar el certificado antiguo.

(6) Si un certificado ha expirado, la restauración del mismo debe de llevarse a cabo como Etapa 2 antes de los seis (06) meses de expirado y la fecha del nuevo ciclo de certificación es con la fecha de otorgamiento del certificado por el comité de certificación.

7.- FORMATOS / REGISTROS

a. Solicitud de Certificación – Renovación (F-CISO-001)
b. Matriz de Clasificación Sectorial (F-CISO-003)
c. Determinación de Tiempos (F-CISO-014)
d. Propuesta de Certificación (F-CISO-005)
e. Acuerdo de Certificación (F-CISO-006)

f. Programa de Auditorías (F-CISO-013)
g. Matriz de Auditores y Consultorías (F-CISO-018)
h. Declaración de Imparcialidad en mis servicios de auditoría (sin código)
i. Plan de Auditoría (F-CISO-012)
j. Verificación de Data Cliente (F-CISO-047)
k. Reporte de Auditoría Etapa 1 (F-CISO-016)
l. Solicitud de Acción Correctiva (F-CISO-015)
m. Reporte de Auditoría Etapa 2 (F-CISO-017)
n. Lista de Verificación (F-CISO 002)
o. Acta de Comité – Certificación (F-CISO-037)

8.- ANEXOS

a. Anexo A: Disposiciones generales para la determinación del tiempo de auditoría.
b. Anexo B: Guía para determinar el tiempo en el proceso de auditoría de certificación a un SGC según la Norma ISO 9001.
c. Anexo C: Guía para determinar el tiempo en el proceso de auditoría de certificación a un SGA según la Norma ISO 14001.
d. Anexo D: Guía para determinar el tiempo en el proceso de auditoría de certificación a un SGSST según la Norma ISO 45001
e. Anexo E: Guía para determinar el tiempo en el proceso de auditoría de certificación a un SGAS según la Norma ISO 37001
f. Anexo F: Guía para determinar el tiempo en el proceso de auditoría de certificación a un SGSI según la Norma ISO/IEC 27001
g. Anexo G: Guía para determinar la reducción o aumento de tiempos de auditorías combinadas
h. Anexo H: Lineamientos de auditoría de Cumplimiento Legal para ISO 45001

9.- CONTROL DE CAMBIOS

Nro.	Descripción	Versión	Fecha
01	- Inclusión de referencias normativas en el procedimiento. - Inclusión de sitios temporales bajo la aprobación del Comité para proceso de Certificación ISO 45001:2018, en la sección de “Decisión de la Certificación – Revisión de la Información”. - Se precisó que una auditoría con notificación a corto plazo también se puede ejecutar por la investigación de Accidentes graves o muertes dentro del SGSST ISO 45001:2018 o si las áreas de trabajo del cliente certificado están sujetas a cierre. - Se precisó que la suspensión o retiro del certificado también puede recaer por incumplimiento legal. - Se ha incluido en el anexo A – Determinación de tiempo de auditoría el inciso Nro. 15. - Se precisó que para ISO 45001:2018 no se aplica muestreo multisio.	09	15-03-2021

	- Se ha incluido en el anexo H – Partes interesadas para el SGSST.		
02	- Se agregó la Norma ISO/IEC 27006:2015/AMD 1:2020 Tecnología de la información - Técnicas de seguridad – Requisitos para entidades que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información.	10	12-07-2021
03	- Se precisó en el apartado 6.a.1.c: cuestionario externo de debida diligencia a terceros (F-CISO-004). - Se precisó responsabilidades a cargo de la Gerencia de Afiliaciones y Fidelización - Se precisó en el Anexo A la nota respecto a turnos. - Se precisó en el apartado 4. Muestreo multisitio ítem C.2 “mismo alcance o similar” para facilitar descuentos.	11	12-01-2023
04	- Se precisó que para las auditorías de seguimiento (excepto la primera auditoría después de la certificación inicial y aquellas cuyo certificado se haya restaurado después de un vencimiento), podrán programarse con dos (02) meses después anualmente, estos cambios en el programa de auditoría deben estar debidamente justificando loas razones. - Se actualizó las referencias de documentos externos	12	08-02-2023
05	- Se retiró la aplicación de la declaración jurada sobre investigaciones y procesos en curso. Se actualizó, que el cuestionario externo de debida diligencia a terceros (F-CISO-004) aplica para el sector privado.	13	18-04-2023
06	- Se actualizó el formato “Declaración de Imparcialidad en mis servicios de auditoría” (sin código)	14	23-06-2023
07	- Se hizo la precisión que Para transiciones de certificación ISO/IEC 27001 se dará cumplimiento a IAF MD 26:2022	15	15-10-2023
08	- Se precisó Declaración de Aplicabilidad (aplica para ISO/IEC 27001), conforme a lo declarado en el reporte de auditoría, en caso la organización realice cambios en la SoA que afectan a la cobertura de los controles, se emitirá un nuevo certificado.	16	08-01-2024
09	- Se precisó que para las auditorías de seguimiento (excepto la primera auditoría después de la certificación inicial y aquellas cuyo certificado se haya restaurado después de un vencimiento), podrán programarse	17	05-03-2024

	con dos (02) meses después de cada vencimiento anual; en el caso se desee ampliar dicho plazo, este no deberá exceder los seis (06) meses después de cada vencimiento anual, los cuales se concederán previa aprobación del Comité de Certificaciones ISO, estos cambios en el programa de auditoría deben estar debidamente justificando las razones.		
10	- Se precisaron los criterios para rechazar una solicitud (pág. 7) - Se incluyo un criterio más para considerar reducir/modificar el alcance de certificación (pág. 27)	18	04-04-2024
11	- Se precisa en el anexo A punto 2 la determinación de puestos efectivos para ISO 37301 y se actualiza en punto 3 y 5 en el anexo G se incluye tabla para determinar días auditor en la Norma ISO 37301.	19	25-11-2024
12	- Se actualizó en el punto de comunicación del plan de auditoría lo siguiente: *El auditor líder comunicará el plan de auditoría al área de SIG con un tiempo no mayor o igual a diez (10) días calendario previo a la auditoría, siempre y cuando la empresa haya enviado su documentación con la debida antelación; de no haber correcciones el área de SIG comunicará al cliente el plan de auditoría al día siguiente hábil de recibir el documento por parte del auditor antes de la auditoría "in situ" o "remota". Para ambos casos, en la medida que se pueda aplicar.* - En el punto de comunicación del reporte de auditoría se actualizó lo siguiente: *El reporte de auditoría final será enviado por el área del SIG al cliente, junto con el(los) formato(s) Solicitud de Acción Correctiva (F-CISO-015),* ***en la medida de lo posible*** *el reporte de auditoría final (de Etapa 2 por certificación o renovación, seguimiento 1 o 2), se enviará al cliente dentro de los 30 (treinta) días calendario posterior al último día de ejecución de la auditoría.*	20	17-03-2025

ANEXO A

DISPOSICIONES GENERALES PARA LA DETERMINACIÓN DEL TIEMPO DE AUDITORÍA

1.- Cálculo para determinar el número de personal efectivo (ISO 9001, ISO 14001, ISO 45001)

Para determinar el número de personal efectivo "X" y punto de partida para la determinación de tiempos de auditoría, se deberá considerar la sumatoria de los siguientes ítems:

1. Total de personas de Alta Dirección a tiempo completo (Responsables de la toma de decisiones, con poder y autoridad y que tienen control sobre la efectividad del Sistema de Gestión). Ej. Gerencias y Jefaturas.
2. Total Personal Administrativo a tiempo completo (Con cierto nivel de autoridad, propios y subcontratados, que realizan actividades similares, continuas, de supervisión, monitoreo y control, dentro del lugar de auditoría y que tienen influencia sobre el Sistema de Gestión), multiplicado por el porcentaje de participación en los turnos diurnos.
3. Raíz cuadrada del número total del personal operativo (propios y subcontratados) a tiempo completo, multiplicado por el porcentaje de participación en los turnos diurnos. (Personas en puestos fijos, rotativos, temporales, que están bajo supervisión, no tienen poder ni autoridad sobre el Sistema de Gestión, realizan actividades similares o repetitivas).
4. Total de personas trabajando a medio tiempo entre el número de horas por turno.

Sólo se podrá aplicar la raíz cuadrada del personal operativo (ítem 3), según documento obligatorio IAF MD5 (cláusula 2.3.4) a las actividades que son repetitivas como: personal de limpieza, seguridad, "call center", entre otros.

Fórmula:

$$X = 1 + 2 + 3 + 4$$

Ejemplo:

1. Personal Alta Dirección (1 turno): 10
2. Personal Administrativo (2 turnos): 60
3. Personal Operativo (Seguridad) (2 turnos): 400
4. Personal Medio Tiempo (4 horas): 5

$$X = 10 + 60*(50\%) + (\sqrt{400}*(50\%)) + (5/4)$$
$$X = 10 + 30 + 10 + 1$$

$$X = 51$$

Nota: *Para el caso anterior se cuenta con 2 turnos, se considera el 50%, ya que en el turno diurno se encuentra la misma proporción de colaboradores que en el turno nocturno.*

2.- Cálculo para determinar el número de puestos efectivos (ISO 37001, ISO 37301)

Para determinar el número de puestos efectivos "X" y punto de partida para la determinación de tiempos de auditoría, se deberá considerar lo siguiente:

Número permanente de empleados	Puestos efectivos
1	1
2	2
3	3
4	4
5 – 100	5
+ de 100	5%

Nota: para determinar los puestos efectivos de las Normas ISO 37001 e ISO 37301 será con base en el alcance certificado y a los procesos relacionados a este, de acuerdo con el análisis del organismo certificador se deberá considerar a los puestos con poder de decisión en relación a los riesgos significativos según sea el caso de antisoborno e incumplimiento del compliance de la organización.

3.- Para la determinación del tiempo de auditoría se tienen en cuenta los siguientes aspectos:

(1) Los requisitos de la norma de sistema de gestión pertinente
(2) Personal/puesto efectivo para el alcance del sistema de gestión pertinente
(3) El tamaño y la complejidad del cliente y de su sistema de gestión
(4) El contexto tecnológico y reglamentario
(5) Toda contratación externa de cualquier actividad incluida en el alcance del sistema de gestión
(6) Los resultados de cualquier auditoría previa
(7) Consideraciones sobre el número de sitios y multisitios
(8) Los riesgos asociados a los procesos o las actividades de la organización.
(9) Si las auditorías son combinadas, conjuntas (otros Organismos de Certificación) o integradas (otras normas)
(10) IAF MD1 (Para el caso de auditorías multisitio basada en el muestreo)
(11) IAF MD5 (Para el caso de SGC ISO 9001, SGA ISO 14001, ISO 37001, SGSST ISO 45001)
(12) IAF MD11 (Para el caso de sistemas integrados de gestión)
(13) Norma ISO/IEC 27006:2015 Tecnología de la información - Técnicas de seguridad – Requisitos para entidades que proporcionan auditoría y certificación de sistemas de gestión de seguridad de la información. (Para el caso de SGSI ISO/IEC 27001)
(14) Otras certificaciones
(15) Para el caso de certificación de SGSST se tendrán en cuenta la auditoria a actividades, productos y servicios dentro del control o influencia de la organización

que puede afectar el desempeño de la SST de la organización, esto incluye sitios de auditoria temporales del cliente de auditoria

4.- Muestreo Auditorías Multisitio

Para auditorías multisitio para una certificación de un cliente, ASOCIACIÓN CIVIL BASC PERÚ ejecuta el programa de muestreo conforme lo establecido en los siguientes párrafos.

a. MULTIPLES LOCALES - METODOLOGÍA DE MUESTREO

(1) La elaboración del presente anexo fue realizada teniendo en cuenta la IAF MD1 para multisitio.

(2) La muestra debe ser parcialmente selectiva basada y debe dar lugar a una gama representativa de diferentes locales de ser seleccionado, sin excluir el elemento aleatorio del muestreo.

(3) Al menos el 25% de la muestra debe ser seleccionada al azar.

(4) La selección del local puede incluir entre otros los siguientes aspectos:

(a) Resultados de revisiones de auditorías previas;
(b) Los registros de quejas y acciones correctivas y preventivas
(c) Variaciones significativas en el tamaño de los locales;
(d) Variaciones en los patrones de cambio y los procedimientos de trabajo;
(e) La complejidad del sistema y los procesos llevados a cabo en los locales de la gestión;
(f) Modificaciones desde la última auditoría de certificación;
(g) La madurez del sistema y el conocimiento de la estructura organizativa;
(h) Las cuestiones ambientales y el alcance de los aspectos e impactos asociados para sistemas ambientales (EMS) de gestión;
(i) Las diferencias en la cultura, el idioma y los requisitos reglamentarios; y
(j) Dispersión geográfica.

Para certificación de SGSST ISO 45001:2018 no aplica el muestreo multisitio y todas las sedes en el alcance de certificación deben ser auditadas, lo anterior justificado en la imposibilidad de ASEGURAR los mismos riesgos de SST e iguales niveles de control y riesgo en los sitios incluidos en el alcance de certificación, todo esto argumentado en la ciencia de gestión de riesgos que establece que para asegurar riesgos similares se tendría que contar con contexto iguales lo que es imposible de lograr según el requisito del IAF MD 22:2019 G 9.1.15 "Aunque un sitio realiza procesos similares o fabrica productos similares a otros sitios, el OC deberá tener en cuenta las diferencias entre las operaciones de cada sitio (tecnología, equipo, cantidades de materiales peligrosos utilizados y almacenados, entorno de trabajo, instalaciones, etc.)."

b. TAMAÑO DE LA MUESTRA

(1) El número mínimo de sitios a ser auditados por visita de auditoría debe ser la raíz cuadrada del número de sitios remotos (y = √ x), redondeado al número entero superior.

(2) La oficina central será auditada durante cada certificación inicial y renovación y anualmente como parte de la vigilancia.

(3) El tamaño o la frecuencia de la muestra obedecen a los siguientes factores y es aplicable para todos los sistemas de gestión acreditados:

(a) El tamaño de los sitios y el número de empleados;
(b) El nivel de complejidad o riesgo de la actividad y del sistema de gestión;
(c) Las variaciones en las prácticas de trabajo (por ejemplo, cambiar de trabajo);
(d) Las variaciones en las actividades emprendidas;
(e) Significado y alcance de los aspectos e impactos asociados para el medio ambiente sistemas de gestión (EMS);
(f) Los registros de quejas y acciones correctivas y preventivas;
(g) Aspectos multinacionales; y
(h) Los resultados de las auditorías internas y revisión por la dirección.
(i) Se permite el muestreo cuando realizan actividades/procesos similares en cada local.

(4) En la solicitud de un grupo nuevo de sitios para unirse a una red multi-sitio ya certificada, cada grupo nuevo de sitios debería considerarse como una serie independiente para la determinación del tamaño de la muestra. Luego de la inclusión del grupo nuevo en el certificado, los sitios nuevos deberían ser acumulados a los anteriores para determinar el tamaño de la muestra para futuras auditorías de seguimiento o de renovación.

(5) Para el caso de la Norma ISO 37301:2021 uno de los criterios para aplicar el muestreo, será asegurar para el caso de empresas del sector privado el cumplimiento de la licencia de funcionamiento de cada local y para el caso del sector público el registro de los locales en registro públicos, SUNAT u otro documento oficial que de manera fehaciente evidencie el local en donde se realizan las actividades.

c. CÁLCULO PARA DÍAS-AUDITOR

(1) El número de días auditor por sitio, incluyendo la oficina central, se debe calcular para cada sitio utilizando el documento IAF para el cálculo de días de acuerdo a la norma pertinente.

(2) Se registrarán las reducciones que pueden aplicar para la oficina central y/o los locales para el cálculo de días auditor mediante el siguiente esquema:

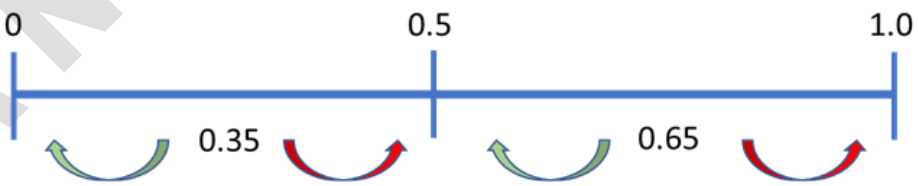
Si la organización Cuenta con:	Solicita mismo alcance o similar
Certificación BASC (posibilidad combinada)	Hasta 30%
1 Certificación ISO	Hasta 20%
2 Certificaciones ISO	Hasta 25%
3 Certificaciones ISO	Hasta 30%

(a) El tiempo determinado de auditoría no contempla tiempos requeridos por miembros del equipo con roles diferentes al de auditor (por ejemplo, expertos técnicos, traductores, interpretes, observadores y auditores en formación).

(b) El tiempo para las auditorías de seguimiento será la tercera parte (1/3) del tiempo total de auditoría inicial.

(c) El número decimal de días auditor final obtenido se redondeará mediante la siguiente regla:

- Si se obtiene un decimal menor o igual a 0.35 se redondeará a 0 día auditor.
- Si se obtiene un decimal mayor o igual a 0.35 pero menor o igual a 0.5 se redondeará a 0.5 día auditor.
- Si se obtiene un decimal mayor o igual a 0.5 pero menor o igual a 0.65 se redondeará a 0.5 día auditor.
- Si se obtiene un decimal mayor o igual a 0.65 pero menor o igual a 1 se redondeará a 1 día auditor



(d) La forma en cómo se determina tiempos para cada norma, así como las reducciones de auditorías combinadas o ampliaciones ya sea por alcance, por incremento de personal quedará evidenciado en el registro Determinación de Tiempos de auditoría. (F-CISO-014).

d. **Para mayor información ver el Anexo 01 formato de código F-CISO-053.**

5.- Auditorías Combinadas / Integradas

a. Se puede decir que una auditoría es combinada cuando se audita bajo los criterios y estándar de más de dos normas al mismo tiempo. El sistema puede estar o no integrado y éste va a depender de qué tan integrada esté la documentación, esto es, cuántos de los requisitos de cada norma está integrado en un mismo documento.

b. El Organismo de Certificación se asegurará de:

(1) Establecer el nivel de integración del sistema (s) de gestión.

(2) Los planes de auditoría deben cubrir todas las áreas y actividades aplicables a cada sistema de gestión, así como el alcance de la auditoría y bajo un auditor competente (s).

(3) La auditoría será administrada por un jefe de equipo, competente en al menos una de las normas auditadas.

(4) Determinar los tiempos de una auditoría.

(5) Justificar los días de reducción o ampliación evidenciándolo con un registro.

(6) La generación de los reportes, pueden ser integrados o separados.

(7) Al establecer no conformidades se deben tener en consideración el impacto que ésta tiene sobre los Sistemas de Gestión.

c. Se debe de confirmar la reducción de tiempos antes y durante la auditoría de Etapa 1.

d. Para determinar la reducción de días, considerar lo indicado en el Anexo G Reducción de Tiempos en Auditorías Combinadas.

ANEXO B

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGC SEGÚN LA NORMA ISO 9001

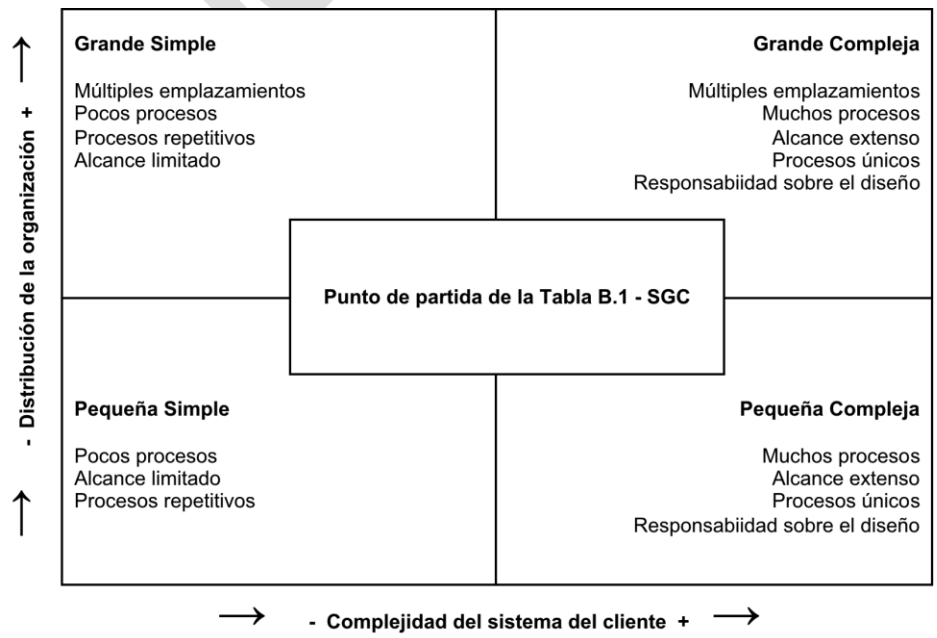
1.- TABLA B.1 - DIAS AUDITOR PARA UN SISTEMA DE GESTION DE LA CALIDAD (SGC)

En esa tabla se especifica el número de días de auditoría de la auditoría inicial (Etapa 1 y Etapa 2) en función del número de empleados y la complejidad y/o riesgos de la organización de acuerdo al IAF MD5.

Tabla B.1 – Número de días auditor para auditoría de certificación inicial – Norma ISO 9001

Número permanente de empleados efectivos	Duración Auditoría Inicial y Certificación (días)	Número permanente de empleados efectivos	Duración Auditoría Inicial y Certificación (días)
1-5	1.5	626-875	12
6-10	2	876-1175	13
11-15	2.5	1176-1550	14
16-25	3	1551-2025	15
26-45	4	2026-2675	16
46-65	5	2676-3450	17
66-85	6	3451-4350	18
86-125	7	4351-5450	19
126-175	8	5451-6800	20
176-275	9	6801-8500	21
276-425	10	8501-10700	22
426-625	11	>10700	Seguimiento progresivo

2.- TABLA B.2 – RELACION ENTRE COMPLEJIDAD Y DURACION DE AUDITORIA



3.- EJEMPLOS DE CATEGORIAS DE RIESGOS

a. Estas categorías de riesgos no son definitivas, son solo ejemplos que se pueden usar a la hora de determinar la categoría de riesgo de una auditoría.

(1) Riesgo Alto. - Cuando un fallo del producto o servicio podría causar daños graves a la organización o a sus clientes.

Los ejemplos incluyen, pero no se limitan a: Alimentación, farmacéutico, aeronaves, construcción naval, elementos y estructuras sometidos a cargas, actividad de construcción compleja, equipos eléctricos y de gas, servicios médicos y de salud, pesca, combustible nuclear, productos químicos y productos químicos y fibras.

(2) Riesgo Medio. - Cuando un fallo del producto o servicio podría causar algunos daños a la organización o a la insatisfacción de sus clientes. Los ejemplos incluyen, pero no se limitan a: Elementos o estructuras no sometidas a carga, actividades de construcción simples, productos metálicos básicos y fabricados, productos no metálicos, mobiliario, equipos ópticos, servicios personales y de ocio.

(3) Riesgo Bajo. - Cuando un fallo del producto o servicio es improbable que cause daños a la organización y a la satisfacción de sus clientes. Los ejemplos incluyen, pero no se limitan a: Sector textil y de confección, fabricación de pasta, papel y productos de papel, edición, servicios de oficina, educación, comercio al por menor y hoteles.

Nota 1: se espera que las actividades de negocio definidas como riesgo bajo, pueden necesitar menos tiempo de auditoría que el calculado usando la tabla B.1, actividades definidas como riesgo medio llevarán el tiempo calculado usando la Tabla B.1, y las actividades definidas como de “riesgo alto” necesitarán más tiempo.

Nota 2: Si una compañía proporciona una mezcla de actividades de negocio, (p.e. compañía de construcción que realiza construcción simple, - riesgo medio- y puentes – alto riesgo), corresponde determinar el tipo de auditoría correcto, teniendo en cuenta el número de personal involucrado en cada una de las actividades.

ANEXO C

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGA SEGÚN LA NORMA ISO 14001

1.- TABLA C.1.- DIAS AUDITOR PARA UN SISTEMA DE GESTION AMBIENTAL (SGA)

En esta tabla se muestra la relación entre el número efectivo de personal, complejidad y duración de la auditoría (únicamente para auditoría inicial)

Número efectivo de empleados	Duración auditoría Etapa 1 + Etapa 2 (Auditor · día)				Número efectivo de empleados	Duración auditoría Etapa 1 + Etapa 2 (Auditor · día)			
	Alto	Medio	Bajo	Limitado		Alto	Medio	Bajo	Limitado
1-5	3	2.5	2.5	2.5	626-875	17	13	10	6.5
6-10	3.5	3	3	3	876-1175	19	15	11	7
11-15	4.5	3.5	3	3	1176-1550	20	16	12	7.5
16-25	5.5	4.5	3.5	3	1551-2025	21	17	12	8
26-45	7	5.5	4	3	2026-2675	23	18	13	8.5
46-65	8	6	4.5	3.5	2676-3450	25	19	14	9
66-85	9	7	5	3.5	3451-4350	27	20	15	10
86-125	11	8	5.5	4	4351-5450	28	21	16	11
126-175	12	9	6	4.5	5451-6800	30	23	17	12
176-275	13	10	7	5	6801-8500	32	25	19	13
276-425	15	11	8	5.5	8501-10700	34	27	20	14
426-625	16	12	9	6	>10700	Seguir la progresión			

Nota 1: Se muestra la duración para auditorías de complejidad alta, media, baja y limitada

Nota 2: El número de empleados en la Tabla C.1 debería ser considerado como un continuo en lugar de un cambio escalonado. Por ejemplo: Si se traza una gráfica, la línea debería empezar con los valores más bajos del intervalo y finalizar en los extremos de cada intervalo. El punto de partida de la gráfica para 1 empleado, debería conllevar 2,5 días. Ver clausula 2.2 para manejar fracciones de día.

2.- TABLA C.2.- Ejemplos de relaciones entre los sectores y las categorías de complejidad de los aspectos ambientales

Categoría de complejidad	Sector
Alta	– Minería e industrias extractivas – Extracción de petróleo y gas – Curtido de pieles y de tejidos – Fabricación de pasta de papel incluyendo el proceso de reciclado de papel – Refino de petróleo – Químicas y farmacéuticas – Metales-Producción primaria – Procesamiento de no metálicos y sus productos cubriendo cerámicos y el cemento – Generación de electricidad basada en el carbón – Construcción civil y demolición – Procesamiento de residuos peligrosos y no peligrosos por ejemplo incineración, etc. – Tratamiento de aguas residuales y vertidos
Media	– Pesca/agricultura/silvicultura – Textiles y ropas excepto el curtido – Fabricación de tableros, tratamiento/impregnación de madera y productos de madera – Producción de papel e impresión exceptuando la fabricación de pasta – Procesamiento de no metálicos y sus productos, cubriendo vidrio, arcilla, cal etc. – Tratamiento superficial y otros tratamientos químicos para productos metálicos manufacturados, excluyendo la producción primaria – Tratamiento superficial y otros tratamientos químicos para maquinaria y equipo mecánico – Producción de circuitos impresos para la industria electrónica – Fabricación de equipo de transporte - carretera, tren, aire, barcos

Categoría de complejidad	Sector
	– Generación y distribución de electricidad que no esté basada en el carbón. – Producción de gas, almacenamiento y distribución (la extracción es de complejidad – Alta) – Captación de agua, purificación y distribución incluyendo gestión de ríos (el – tratamiento comercial de vertidos es de complejidad Alta) – Venta al por mayor y al por menor de combustible fósil – Fabricación de comida y tabaco – Transporte y distribución - por mar, aire, tierra – Agencias de comercio inmobiliario, gestión inmobiliaria, limpieza industrial, limpieza higiénica, limpieza en seco, normalmente son parte de los servicios generales – Reciclado, compostaje, y vertedero (de residuos no peligrosos) – Ensayos técnicos y laboratorios – Cuidado de la salud/hospitales/veterinaria – Servicios de ocio y servicios personales excluyendo hoteles y restaurantes
Baja	– Hoteles/restaurantes – Madera, productos de madera, excluyendo la fabricación de tableros, el tratamiento y – la impregnación de madera – Productos de papel excluyendo impresión, pasta de papel y fabricación de papel – Moldeado por inyección de goma y plástico. Conformado y ensamblaje. Excluye la fabricación de materias primas de goma y plástico que son parte de Química – Moldeado en caliente y en frío y fabricación de metal excluyendo tratamiento de superficie y otros tratamientos químicos y producción primaria – Ensamblaje de maquinaria y equipo mecánicos excluyendo tratamiento de superficie y otros tratamientos químicamente basados – Venta al por mayor y al por menor – Ensamblaje de equipo eléctrico y electrónico excluyendo la fabricación de tableros de circuitos impresos
Limitada	– Actividades corporativas y de gestión, sedes centrales y gestión de sociedades – Transporte y distribución – únicamente servicios de gestión, sin una flota real – Telecomunicaciones – Servicios generales a los negocios exceptuando las agencias de comercio inmobiliario, gestión inmobiliaria, limpieza industrial, limpieza higiénica y limpieza en seco – Servicios de enseñanza/educación
Casos especiales	– Nuclear – Generación nuclear de electricidad – Almacenamiento de grandes cantidades de material peligroso – Administración pública – Autoridades locales – Organizaciones con productos o servicios ambientalmente sensibles – Instituciones financieras

a. CATEGORÍAS DE COMPLEJIDAD DE LOS ASPECTOS AMBIENTALES

(1) Estas directrices se basan en cuatro categorías primarias de complejidad de la naturaleza, número y gravedad de los aspectos ambientales de una organización que afectan fundamentalmente al tiempo de auditor. Estas son:

(a) Alta: aspectos ambientales con naturaleza y gravedad importante (organizaciones de fabricación o procesamiento con impactos significativos en varios aspectos ambientales).

(b) Media: aspectos ambientales con naturaleza y gravedad media (organizaciones de fabricación o procesamiento con impactos significativos en algunos aspectos ambientales).

(c) Baja: aspectos ambientales con una naturaleza y gravedad baja (organizaciones de fabricación o procesamiento con impactos significativos en pocos aspectos ambientales).

(d) Limitada: aspectos ambientales con una naturaleza y gravedad limitada (organizaciones del tipo de oficinas). Especial: estas requieren consideración adicional y única en la etapa de planificación de la auditoría.

(2) La Tabla C.1 cubre las cuatro principales categorías de complejidad: alta, media, baja y limitada.

(3) La Tabla C.2 proporciona la relación entre las cinco categorías de complejidad y los sectores que podrían típicamente estar en cada categoría.

(4) ASOCIACION CIVIL BASC PERU reconoce que no todas las organizaciones de un sector determinado estarán siempre en la misma categoría de complejidad. Para lo cual en el momento de revisar la solicitud debe asegurarse que las actividades específicas de la organización son consideradas para determinar la categoría de complejidad. Por ejemplo: aunque muchos negocios en el sector químico se clasificarían como de complejidad "alta", una organización que se limita a formular sin llevar a cabo reacciones químicas o emisiones y/o comercialización podría clasificarse como "medio" e incluso "baja complejidad". Para lo cual documenta todos los casos en los que se fijan categorías de complejidad más bajas para una organización en un sector específico.

(5) La tabla C.1 no cubre la categoría especial y los tiempos de auditoría deberán justificarse y desarrollarse individualmente en estos casos.

ANEXO D

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGSST SEGÚN LA NORMA ISO 45001

1.- TABLA D.1.- DIAS AUDITOR PARA UN SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO (SGSST)

Relación entre el número efectivo de personal, la categoría de complejidad del riesgo para la SST y el tiempo de auditoría (únicamente para auditoría inicial etapa 1 + etapa 2)

Número efectivo de empleados	Duración auditoría Etapa 1 + Etapa 2 (Auditor · día)			Número efectivo de empleados	Duración auditoría Etapa 1 + Etapa 2 (Auditor · día)		
	Alto	Medio	Bajo		Alto	Medio	Bajo
1-5	3	2.5	2.5	626-875	17	13	10
6-10	3.5	3	3	876-1175	19	15	11
11-15	4.5	3.5	3	1176-1550	20	16	12
16-25	5.5	4.5	3.5	1551-2025	21	17	12
26-45	7	5.5	4	2026-2675	23	18	13
46-65	8	6	4.5	2676-3450	25	19	14
66-85	9	7	5	3451-4350	27	20	15
86-125	11	8	5.5	4351-5450	28	21	16
126-175	12	9	6	5451-6800	30	23	17
176-275	13	10	7	6801-8500	32	25	19
276-425	15	11	8	8501-10700	34	27	20
426-625	16	12	9	>10700	Seguir la progresión		

2.- TABLA D.2 – EJEMPLOS DE RELACIONES ENTRE LOS SECTORES Y LAS CATEGORÍAS DE COMPLEJIDAD DE LOS RIESGOS PARA LA SST

Categoría de complejidad	Sector
Alta	– Pesca (en el mar, el dragado de la costa y el buceo). – Minería e industria extractiva. – Extracción de petróleo y gas. – Curtido de pieles y de tejidos. – Fabricación de pasta de papel incluyendo el proceso de reciclado de papel. – Refino de petróleo. – Industria química (incluidos plaguicidas y fabricación de pilas y acumuladores) y farmacéutica. – La fabricación de fibra de vidrio. – La producción, almacenamiento y distribución de gas. – Generación y distribución de electricidad. – Nuclear. – Almacenamiento de grandes cantidades de material peligroso. – Procesamiento de no metálicos y sus productos cubriendo cerámicos y el cemento. – Producción primaria de metales. – Conformado en caliente y frío y fabricación de productos metálicos. – Fabricación y montaje de estructuras metálicas. – Astilleros (dependiendo de las actividades puede ser de complejidad media). – Industria aeroespacial. – Industria del automóvil. – Fabricación de armas y explosivos. – Reciclaje de residuos peligrosos. – Tratamiento de residuos peligrosos y no peligrosos (por ejemplo, incineración). – Tratamiento de aguas residuales y vertidos. – Construcción civil e industrial (incluyendo actividades de acabado de edificios: instalaciones eléctricas, hidráulicas y de aire acondicionado) y demolición. – Mataderos. – Transporte y distribución de mercancías peligrosas (por tierra, aire y agua). – Actividades de defensa y de gestión de crisis. – Cuidado de la salud, hospitales, actividades veterinarias y trabajos sociales.

Categoría de complejidad	Sector
Media	– Acuicultura (cría, engorde y recolección de animales y plantas en todo tipo de ambientes de agua). – Pesca (la pesca en el mar es de complejidad alta). – Ganadería y silvicultura (dependiendo de las actividades puede ser de complejidad alta). – Producción de alimentos, bebidas y tabaco. – Textiles y ropas excepto el curtido. – Fabricación de tableros, tratamiento/impregnación de madera y productos de madera. – Producción de papel e impresión exceptuando la fabricación de pasta. – Procesamiento de no metálicos y sus productos, cubriendo vidrio, arcilla, cal, etc. – Montaje mecánico en general. – Fabricación de productos metálicos. – Tratamiento superficial y otros tratamientos químicos para productos metálicos manufacturados, excluyendo la producción primaria y el montaje mecánico (dependiendo del tratamiento y del tamaño de componente las actividades pueden ser de complejidad alta). – Producción de circuitos de impresos para la industria electrónica. – Moldeado por inyección de goma y plástico. Conformado y ensamblaje. – Montaje de equipos eléctricos y electrónicos. – Fabricación y reparación de equipos de transporte por carretera, tren y aire (dependiendo del tamaño del equipo puede ser de complejidad alta). – Reciclado, compostaje y vertedero (de residuos no peligrosos). – Captación de agua, purificación y distribución incluyendo gestión de ríos (el tratamiento de vertidos es de complejidad alta). – Venta al por mayor y al por menor de combustible fósil (dependiendo de la cantidad de combustible puede ser de complejidad alta). – Transporte y distribución de mercancías no peligrosas (por tierra, aire y agua). – Servicios de limpieza industrial, limpieza higiénica o limpieza en seco, normalmente parte de los servicios de reciclado, el compostaje y los vertederos (de los residuos no peligrosos). – Investigación y desarrollo en ciencias naturales y técnicas (en función del sector de actividad podría ser alta). Ensayos técnicos y laboratorios. – Hoteles, servicios de ocio y servicios personales excluyendo restaurantes. – Actividades de educación (en función del objetivo de las actividades de enseñanza podrían ser de complejidad alta o baja).
Baja	– Actividades corporativas y de gestión, sedes centrales y gestión de sociedades. – Venta al por mayor y al por menor (dependiendo del producto puede ser de complejidad media o alta, por ejemplo, combustible). – Servicios generales a los negocios exceptuando limpieza industrial, limpieza higiénica y limpieza en seco y servicios de educación. – Transporte y distribución – únicamente servicios de gestión, sin una flota real. – Servicios de ingeniería (dependiendo del tipo de servicios podría ser de complejidad media). – Telecomunicaciones y servicios postales. □ – Restaurantes y campings. – Agencias de comercio inmobiliario y gestión inmobiliaria. – Investigación y desarrollo en ciencias sociales y humanidades. – Administración pública y autoridades locales. – Instituciones financieras y agencias de publicidad.

a. CATEGORÍAS DE COMPLEJIDAD DE LOS RIESGOS DE SST

(1) Estas directrices se basan en tres categorías primarias de complejidad de los riesgos para la seguridad y salud de los trabajadores, basadas en la naturaleza y gravedad de los riesgos de una organización, que afectan fundamentalmente al tiempo de auditor. Estas son:

(a) Alta: riesgos con naturaleza y gravedad importante (empresas constructoras, industria pesada o empresas de fabricación son típicas de esta categoría).

(b) Media: riesgos con naturaleza y gravedad media (empresas de industria ligera con algunos riesgos importantes, son típicas de esta categoría).

(c) Baja: riesgos con naturaleza y gravedad baja (organizaciones que desarrollan su actividad desde oficinas son típicas de esta categoría).

(2) La Tabla D.1 cubre las tres categorías de complejidad del riesgo para la seguridad y salud de los trabajadores.

(3) La Tabla D.2 proporciona la relación entre las tres categorías de complejidad del riesgo y los sectores que podrían típicamente estar en cada categoría.

(4) ASOCIACION CIVIL BASC PERU reconoce que no todas las organizaciones de un sector determinado estarán siempre en la misma categoría de complejidad del riesgo. En la revisión de la solicitud de certificación se consideran las actividades específicas de la organización para determinar la categoría de complejidad. Por ejemplo: aunque muchos negocios en el sector de la construcción naval se clasificarían como de complejidad "alta", una organización que se limita a fabricar pequeñas embarcaciones de fibra de carbono con actividades de menor complejidad, podría clasificarse como de complejidad "media". Se debe documentar todos los casos en los que se asocien categorías de complejidad más bajas para una organización en un sector específico.

(5) Nota: la categoría de complejidad de los riesgos para la seguridad y salud de los trabajadores de una organización, se puede asociar también a las consecuencias de un fallo en la capacidad del SGSST para controlar el riesgo:

(a) Alto - donde un fallo en la gestión del riesgo podría poner en riesgo la vida o causar lesiones graves.

(b) Medio - donde un fallo en la gestión del riesgo podría resultar en una lesión o enfermedad.

(c) Baja – donde un fallo en la gestión del riesgo puede resultar en lesiones o enfermedades menores.

ANEXO E

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGAS SEGÚN LA NORMA ISO 37001

1.- TABLA E.1 - DIAS AUDITOR PARA UN SISTEMA DE GESTION ANTISOBORNO (SGAS)

En esa tabla se especifica el número de días para la auditoría inicial (Etapa 1 y Etapa 2) en función del número de puestos y la complejidad y/o riesgos de la organización.

Tabla E.1 – Número de días auditor para auditoría de certificación inicial – Norma ISO 37001

Número permanente de puestos efectivos	Duración Auditoría Inicial y Certificación (días)	Número permanente de puestos efectivos	Duración Auditoría Inicial y Certificación (días)
1-5	1.5	626-875	12
6-10	2	876-1175	13
11-15	2.5	1176-1550	14
16-25	3	1551-2025	15
26-45	4	2026-2675	16
46-65	5	2676-3450	17
66-85	6	3451-4350	18
86-125	7	4351-5450	19
126-175	8	5451-6800	20
176-275	9	6801-8500	21
276-425	10	8501-10700	22
426-625	11	>10700	Seguimiento progresivo

ANEXO F

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGSI SEGÚN LA NORMA ISO/IEC 27001

1.- TABLA F.1 - DIAS AUDITOR PARA UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

En esta tabla se especifica el número de días para la auditoría inicial (Etapa 1 y Etapa 2) en función del número de empleados y la complejidad y/o riesgos de la organización de acuerdo a la norma ISO/IEC 27006.

Tabla F.1 – Número de días auditor para auditoría de certificación inicial – Norma ISO 27001

Número de personas que realizan trabajo bajo el control de la organización.	Duración Auditoría Inicial y Certificación (días)	Número de personas que realizan trabajo bajo el control de la organización.	Duración Auditoría Inicial y Certificación (días)
1-10	5	876-1175	18.5
11-15	6	1176-1550	19.5
16-25	7	1551-2025	21
26-45	8.5	2026-2675	22
46-65	10	2676-3450	23
66-85	11	3451-4350	24
86-125	12	4351-5450	25
126-175	13	5451-6800	26
176-275	14	6801-8500	27
276-425	15	8501-10700	28
426-625	16.5	>10700	Seguimiento progresivo
626-875	17.5		

2.- Tabla F.2 - Clasificación de factores para el cálculo del tiempo de auditoría.

Factores	Impacto sobre el esfuerzo		
	Esfuerzo reducido	Esfuerzo normal	Esfuerzo mayor
a) complejidad del SGSI: • requisitos de seguridad de la información. [confidencialidad, integridad y disponibilidad, (CIA)] • número de activos críticos • número de procesos y servicios.	• Solo poca información sensible o confidencial, requisitos de baja disponibilidad. • Pocos activos críticos (en términos de la CIA) • Solo un proceso de negocio clave con pocas interfaces y pocas unidades de negocio involucradas	• Mayores requisitos de disponibilidad o información confidencial / confidencial. • Algunos activos críticos • 2–3 procesos de negocio simples con pocas interfaces y pocas unidades de negocio involucradas	• Mayor cantidad de información sensible o confidencial (por ejemplo, salud, información de identificación personal, seguro, banca) o requisitos de alta disponibilidad. Muchos activos críticos • Más de 2 procesos complejos con muchas interfaces y unidades de negocio involucradas
b) el tipo de negocio realizado dentro del alcance del SGSI	• Negocio de bajo riesgo sin requerimientos regulatorios.	• Altos requisitos reglamentarios	• Negocio de alto riesgo con (solo) requisitos regulatorios limitados

Factores	Impacto sobre el esfuerzo		
	Esfuerzo reducido	Esfuerzo normal	Esfuerzo mayor
c) desempeño previamente demostrado del SGSI	• Certificado recientemente • No está certificado, pero SGSI se implementó completamente en varios ciclos de auditoría y mejora, incluidas auditorías internas documentadas, revisiones de gestión y un sistema de mejora continua efectivo.	• Auditoría de vigilancia reciente • SGSI no certificado, pero parcialmente implementado: algunas herramientas del sistema de gestión están disponibles e implementadas; Algunos procesos de mejora continua están implementados, pero parcialmente documentados.	• Sin certificación y sin auditorías recientes • SGSI es nuevo y no está completamente establecido (por ejemplo, falta de mecanismos de control específicos del sistema de gestión, procesos de mejora continua inmaduros, ejecución de procesos ad hoc)
d) el alcance y la diversidad de la tecnología utilizada en la implementación de los diversos componentes del SGSI (por ejemplo, número de plataformas informáticas diferentes, número de redes segregadas)	• Entorno altamente estandarizado con poca diversidad (pocas plataformas de TI, servidores, sistemas operativos, bases de datos, redes, etc.)	• Plataformas de TI estandarizadas pero diversas, servidores, sistemas operativos, bases de datos, redes	• Alta diversidad o complejidad de TI (por ejemplo, muchos segmentos diferentes de redes, tipos de servidores o bases de datos, número de aplicaciones clave)
e) el alcance de la subcontratación y los acuerdos con terceros utilizados en el ámbito de la SGSI.	• Sin externalización y poca dependencia de los proveedores, o • Acuerdos de subcontratación bien definidos, gestionados y supervisados. • Outsourcer cuenta con un certificado SGSI. • Los informes de aseguramiento indep. relevantes están disponibles	• Varios acuerdos de subcontratación parcialmente gestionados.	• Alta dependencia de la externalización o proveedores con gran impacto en actividades comerciales importantes, o • Cantidad o extensión desconocida de la subcontratación, o • Varios acuerdos de subcontratación no gestionados
f) alcance del desarrollo del sistema de información.	• No hay desarrollo interno del sistema • Uso de plataformas de software estandarizadas.	• Uso de plataformas de software estandarizadas con configuración / parametrización compleja • Software (altamente) personalizado • Algunas actividades de desarrollo (internas o externas)	• Amplias actividades de desarrollo de software interno con varios proyectos en curso para propósitos comerciales importantes
g) número de sitios y número de sitios de recuperación de desastres (RD)	• Requisitos de baja disponibilidad y ningún sitio RD alternativo.	• Requisitos de disponibilidad media o alta y ningún sitio RD alternativo	• Requisitos de alta disponibilidad, por ej. Servicios 24/7 • Varios sitios RD alternativos • Varios centros de datos

Factores	Impacto sobre el esfuerzo		
	Esfuerzo reducido	Esfuerzo normal	Esfuerzo mayor
h) para la auditoría de vigilancia o renovación: la cantidad y el alcance del cambio relevante para el SGSI de acuerdo con ISO / IEC 17021-1, 8.5.3	• No hay cambios desde la última auditoría de renovación.	• Cambios menores en el alcance o SoA de SGSI, p. Ej. Algunas políticas, documentos, etc. • Cambios menores en los factores anteriores.	• Cambios importantes en el alcance o SoA de SGSI, p. Ej. Nuevos procesos, nuevas unidades de negocio, áreas, metodología de gestión de evaluación de riesgos, políticas, documentación, tratamiento de riesgos. • Cambios importantes en los factores anteriores.

3.- Tabla F.3 - Factores relacionados con la empresa y la organización (que no sean TI)

Categoría	Grado
Tipo(s) de negocio y requisitos reglamentarios.	1. La organización trabaja en sectores comerciales no críticos y sectores no regulados **(*)** 2. La organización tiene clientes en sectores críticos de negocios **(*)** 3. La organización trabaja en sectores empresariales críticos **(**)**
Procesos y tareas	1. Procesos estándar con tareas estándar y repetitivas; muchas personas que realizan trabajos bajo el control de la organización que realizan las mismas tareas; pocos productos o servicios 2. Procesos estándar pero no repetitivos, con alto número de productos o servicios. 3. Procesos complejos, gran cantidad de productos y servicios, muchas unidades de negocios incluidas en el alcance de la certificación (SGSI cubre procesos altamente complejos o un número relativamente alto o actividades únicas)
(*) Los sectores empresariales críticos son sectores que pueden afectar los servicios públicos críticos que causarán riesgos para la salud, la seguridad, la economía, la imagen y la capacidad del gobierno para funcionar, lo que puede tener un gran impacto negativo en el país.	
Nivel de establecimiento de la MS	1. SGSI ya está bien establecido y / u otros sistemas de gestión están en su lugar 2. Se implementan algunos elementos de otros sistemas de gestión, otros no 3. Ningún otro sistema de gestión implementado, el SGSI es nuevo y no está establecido
(**) Los sectores empresariales, la economía, la imagen y la capacidad del gobierno para funcionar, lo que puede tener un gran impacto negativo en el país.	

4.- Tabla F.4 - Factores relacionados con el entorno informático.

Categoría	Grado
Complejidad de la infraestructura de TI	1. Pocas o altamente estandarizadas plataformas de TI, servidores, sistemas operativos, bases de datos, redes, etc. 2. Varias plataformas de TI, servidores, sistemas operativos, bases de datos, redes diferentes. 3. Muchas plataformas de TI, servidores, sistemas operativos, bases de datos, redes diferentes.
Dependencia de la externalización y los proveedores, incluidos los servicios en la nube.	1. Poca o nula dependencia de la subcontratación o de los proveedores. 2. Alguna dependencia de la subcontratación o los proveedores, relacionada con algunas, pero no todas las actividades comerciales importantes 3. Alta dependencia de la subcontratación o de los proveedores, gran impacto en importantes actividades de negocios.

Categoría	Grado
Desarrollo del sistema de información	1. Ninguno o un sistema interno / desarrollo de aplicaciones muy limitado. 2. Algunos desarrollos internos o externos de sistemas / aplicaciones para algunos propósitos comerciales importantes. 3. Amplio desarrollo de aplicaciones / sistemas internos o externos para importantes propósitos comerciales.

5.- Tabla F.5 - Impacto de los factores sobre el tiempo de auditoría.

		Complejidad de TI		
		Bajo (de 3 a 4)	**Medio (de 5 a 6)**	**Alto (de 7 a 9)**
Complejidad empresarial	**Alto (de 7 a 9)**	+5 % a +20 %	+10 % a +50 %	+20 % a +100 %
	Medio (de 5 a 6)	-5 % a −10 %	0 %	+10 % a +50 %
	Bajo (de 3 a 4)	-10 % a −30 %	-5 % a −10 %	+5 % a +20 %

6.- Ejemplo para el cálculo del tiempo de auditoría

El siguiente ejemplo ilustra cómo un organismo de certificación puede usar los factores proporcionados en las tablas F para calcular el tiempo de auditoría. El cálculo del tiempo de auditoría en el siguiente ejemplo funciona de la siguiente manera:

Paso 1: Determinación de los factores relacionados con el negocio y la organización (que no sean TI): identifique la calificación adecuada para cada una de las categorías que figuran en la Tabla F.3 y resuma los resultados.

Paso 2: Determinación de los factores relacionados con el entorno de TI: identifique el grado adecuado para cada una de las categorías que figuran en la Tabla F.4 y resuma los resultados.

Paso 3: Con base en los resultados de los pasos 1 y 2 anteriores, identifique el impacto de los factores en el tiempo de auditoría seleccionando la entrada apropiada en la Tabla F.5.

Paso 4: Cálculo final: el número de días determinado al aplicar el cuadro de tiempo de auditoría (Tabla F.1) se multiplica por el factor resultante del Paso 3. Cuando se utiliza el muestreo en múltiples sitios, los días de auditoría calculados se incrementan en función del esfuerzo necesario para ejecutar el plan de muestreo de sitios múltiples.
Este resultado es el número final de días de auditoría.

EJEMPLO 1 La organización que se auditará tiene 700 empleados, por lo que de acuerdo con la Tabla F.1, se requieren 17.5 días para la auditoría inicial.

La organización no trabaja en un sector empresarial crítico, tiene tareas altamente estandarizadas y repetitivas y acaba de establecer el SGSI.

De acuerdo con la Tabla F.3, esto generaría un factor relacionado con el negocio y la organización de 1 + 1 + 3 = 5. La organización tiene muy pocas plataformas de TI y bases de datos, pero utiliza la subcontratación extensivamente. No hay desarrollo dentro de la organización o subcontratados. De acuerdo con la Tabla F.4, esto generaría un factor relacionado con el entorno de TI de 1 + 3 + 1 = 5. El uso de la Tabla F.5 no generaría ningún ajuste por el tiempo de auditoría.

EJEMPLO 2 La misma organización que en el ejemplo anterior, excepto que ya existen varios sistemas de administración y el SGSI ya está bien establecido. Esto cambiaría el cálculo de acuerdo con la Tabla F.3 a 1 + 1 + 1 = 3. Según la Tabla F.5, esto produciría una reducción del 5% al 10% del tiempo de auditoría, es decir, el tiempo de auditoría se reduciría en 1 día a 1.5 días, con un total de 16 a 16.5 días.

Ver aplicación en registro del SIG F-CISO-014 con Anexo 1.

ANEXO G

GUÍA PARA DETERMINAR EL TIEMPO EN EL PROCESO DE AUDITORÍA DE CERTIFICACIÓN A UN SGC SEGÚN LA NORMA ISO 37301

7.- TABLA E.1 - DIAS AUDITOR PARA UN SISTEMA DE GESTION DE COMPLIANCE (SGC)

En esa tabla se especifica el número de días para la auditoría inicial (Etapa 1 y Etapa 2) en función del número de puestos y la complejidad y/o riesgos de la organización relacionados al compliance.

Tabla E.1 – Número de días auditor para auditoría de certificación inicial – Norma ISO 37301

Número permanente de puestos efectivos	Duración Auditoría Inicial y Certificación (días)	Número permanente de puestos efectivos	Duración Auditoría Inicial y Certificación (días)
1-5	1.5	626-875	12
6-10	2	876-1175	13
11-15	2.5	1176-1550	14
16-25	3	1551-2025	15
26-45	4	2026-2675	16
46-65	5	2676-3450	17
66-85	6	3451-4350	18
86-125	7	4351-5450	19
126-175	8	5451-6800	20
176-275	9	6801-8500	21
276-425	10	8501-10700	22
426-625	11	>10700	Seguimiento progresivo

ANEXO H

GUÍA PARA DETERMINAR LA REDUCCION O AUMENTO DE TIEMPOS DE AUDITORIAS COMBINADAS / INTEGRADAS (MD 11)

1. Tipos de enfoques de auditoría

1.1. Método estándar de auditoría de los sistemas integrados de gestión

a) La auditoría será realizada por uno o más auditores.
b) Los auditores están cualificados para una o más normas/especificaciones del sistema de gestión relevantes para el alcance de la auditoría.

1.2. Enfoque de auditoría ampliada (EAA) de los sistemas integrados de gestión

a) El EAA es aplicable únicamente a las organizaciones con sistemas de gestión plenamente integrados (véanse los criterios en el Anexo 2 – 6.2).
b) La auditoría será realizada por uno o más auditores.
c) Los auditores están cualificados para una o más normas/especificaciones del sistema de gestión relevantes para el alcance de la auditoría.
d) El EAA emplea una sesión de planificación obligatoria previa a la auditoría (véase el anexo 1 – 6.1) por parte del auditor principal.
e) El auditor principal sólo auditará las cláusulas 4, 5, 6, 9 y 10 (de las normas/especificaciones del sistema de gestión con arreglo a la estructura de alto nivel) del Sistema de Gestión Integrado.

Nota: Se entiende por criterios de auditoría las normas de sistemas de gestión utilizadas como base para la evaluación y certificación de la conformidad (por ejemplo, ISO 9001, ISO 14001, ISO/IEC 20000, ISO 22000, ISO/IEC 27001, etc.).

2. Aplicación

2.1. El Organismo de Certificación identificará el enfoque a aplicar 1.1 o 1.2 y se asegurará de:

2.1.1 Al establecer el programa de auditoría se tiene en cuenta el nivel de integración del sistema o sistemas de gestión.
2.1.2 Los planes de auditoría cubren todas las áreas y actividades aplicables a cada norma/especificación del sistema de gestión cubierta por el alcance de la auditoría.
2.1.3 El equipo de auditoría en su conjunto deberá satisfacer los requisitos de competencia, establecidos por el Organismo de Certificación, para cada área técnica, según sea relevante para cada norma/especificación del sistema de gestión cubierta por el alcance de la auditoría de un SIG.
2.1.4 La auditoría será dirigida por un jefe de equipo, competente en al menos una de las normas/especificaciones auditadas (ISO/IEC 17021-1:2015 Nota en 9.2.2.1.2). Cuando se utilice el método de auditoría ampliada (EAA), el jefe del equipo de auditoría tendrá competencias adicionales en la aplicación de la metodología de las EAA (anexo 1 – 6.1).
2.1.5 Se asignará tiempo suficiente para llevar a cabo una auditoría completa y efectiva del sistema de gestión de la organización para las normas/especificaciones del sistema de gestión cubiertas por el alcance de la auditoría.

2.2. Enfoque estándar de auditoría: Para determinar el tiempo de auditoría de un SIG que cubra dos o más normas/especificaciones del sistema de gestión, por ejemplo, A + B + C, el Organismo de Certificación deberá:

a) calcular por separado el tiempo de auditoría requerido para cada norma/especificación del sistema de gestión (aplicando todos los factores pertinentes previstos en los documentos de

aplicación y/o las reglas del esquema pertinentes para cada norma, por ejemplo, IAF MD 4, IAF MD5, ISO/TS 22003, ISO/IEC 27006);

b) calcular el punto de partida T para la duración de la auditoría del SIF sumando la suma de las partes individuales (por ejemplo, T = A + B + C);

c) ajustar la cifra del punto de partida teniendo en cuenta los factores que pueden aumentar o reducir (véase el anexo 2 – 6.2) el tiempo necesario para la auditoría.

Los factores de reducción incluirán, pero no se limitarán a:

i. La medida en que el sistema de gestión de la organización es integrado;
ii. La capacidad del personal de la organización para responder a preguntas relativas a más de una norma de sistemas de gestión; y
iii. La disponibilidad de uno o más auditores competentes para auditar más de una norma o especificación del sistema de gestión.

Los factores de los aumentos incluirán, entre otros:

i. La complejidad de la auditoría de un SGI en comparación con las auditorías de un único sistema de gestión.

d) informar al cliente de que la duración de una auditoría integrada basada en el nivel declarado de integración del sistema de gestión de la organización puede ser objeto de ajustes sobre la base de la confirmación del nivel de integración en la fase 1 y en auditorías posteriores.

2.2.1. La auditoría de un SGI podría resultar en un aumento del tiempo, pero si resulta en una reducción, no deberá exceder el 20% desde el punto de partida T (2.2.b).

2.3. Enfoque de auditoría ampliada: Determinar el tiempo de auditoría para una auditoría de un SGI que abarque dos o más normas/especificaciones de sistemas de gestión, utilizando el Método de auditoría ampliada:

a) calcular por separado el tiempo de auditoría requerido para cada norma/especificación del sistema de gestión (aplicando todos los factores pertinentes previstos en los documentos de aplicación y/o las reglas del esquema pertinentes para cada norma, por ejemplo, IAF MD 4, IAF MD5, ISO/TS 22003, ISO/IEC 27006);
b) tomar el tiempo de auditoría más largo para una sola norma del IMS y luego sumar el 50% del tiempo de auditoría de cada norma adicional T = A + 0,5 B + 0,5 C + ... con A > B y C; y
c) la confirmación final de la duración de la auditoría se realiza en la sesión de planificación (2.4), sin embargo, no será inferior a la obtenida aplicando la metodología de los puntos anteriores.

2.4. Los documentos de solicitud existentes (por ejemplo, los documentos obligatorios de la IAF) relativos a las auditorías de las normas/especificaciones de los sistemas de gestión deben tenerse en cuenta a la hora de elaborar el programa de auditoría y los planes de auditoría para un SGI. Si se toma EAA, es necesario llevar a cabo una sesión de planificación con el cliente para entender completamente el sistema de gestión integrado y su nivel de integración (parte del 20 por ciento del tiempo fuera de las instalaciones puede utilizarse para esta sesión de planificación). Se llevarán registros de la sesión de planificación.

2.5. Se auditarán todos los requisitos aplicables de cada norma/especificación del sistema de gestión que sea pertinente para el alcance del SGI.

2.6. Se documentará el punto de partida para determinar el tiempo de auditoría y la justificación del aumento o la reducción.

2.7. Los informes de auditoría se integrarán para ambos enfoques, a menos que se exija otra cosa, con respecto a los sistemas de gestión auditados. Cada incidencia planteada en un informe integrado deberá poder rastrearse hasta la(s) norma(s)/especificación(es) aplicable(s) al sistema de gestión.

2.8. El Organismo de Certificación considerará el impacto que una no conformidad encontrada para una norma/especificación de un sistema de gestión tiene en el cumplimiento de la(s) otra(s) norma(s)/especificación(es) de otro(s) sistema(s) de gestión. Si la organización no cumple uno de los requisitos comunes del SGI, la no conformidad es aplicable a todo el SGI. Si la organización no cumple con un requisito específico de una norma, entonces impacta al SGI en lo que respecta a esa norma solamente.

2.9. El Organismo de Certificación considerará el método de cálculo para las auditorías de múltiples sitios (MD 1, sección 6), cuando realice auditorías de múltiples sitios.

3. AUDITORÍA Y CERTIFICACIÓN INICIALES

3.1. Solicitud del cliente
Deberá incluir la información relativa al nivel de integración del sistema de gestión, de la documentación, los elementos del SG y las responsabilidades (véase el anexo 2 – 6.2).

3.2. Etapa 1 - Auditoría
Durante la auditoría de etapa 1, el equipo de auditoría confirmará el nivel de integración del SG y el resultado de la sesión de planificación en el caso de las EAA (2.3). El auditor principal confirmará el nivel de integración (véase el anexo 1 – 6.1). El Organismo de Certificación tendrá un proceso para revisar y modificar, según sea necesario, la duración de la auditoría que se basó en la información proporcionada en la etapa de solicitud.

4. ACTIVIDADES DE VIGILANCIA Y RENOVACIÓN

ASOCIACIÓN CIVIL BASC PERÚ confirmará que el nivel de integración permanece inalterado a lo largo del ciclo de certificación para asegurar que las duraciones de auditoría establecidas siguen siendo aplicables. Los detalles de esta confirmación se incluirán en los registros de auditoría.

5. SUSPENSIÓN, REDUCCIÓN, RETIRADA

Si la certificación de una o más normas/especificaciones del sistema de gestión está sujeta a suspensión, reducción o retirada, el Organismo de Certificación investigará el impacto de esto en la certificación de otras normas/especificaciones del sistema de gestión.

6. ANEXOS

6.1. ANEXO 1 - ENFOQUE DE AUDITORÍA AMPLIADA

El EAA requiere una sesión de planificación avanzada con el cliente antes de la determinación final del tiempo de auditoría y la estructuración efectiva del plan de auditoría de acuerdo con los procesos, el SGI y la estructura del cliente.

Concluir en la etapa 1 que los EAA son elegibles mediante la revisión de la misma:

- Los objetivos que deben alcanzarse en uno de los aspectos del rendimiento organizativo (por ejemplo, medioambiental) no afectarán negativamente a la consecución de los objetivos de los otros aspectos (por ejemplo, la calidad); y
- Los asuntos externos e internos que afectan la capacidad de lograr los resultados previstos de cada aspecto del desempeño organizacional que el SGI está gestionando no están contrarrestando el logro de resultados en otro conjunto de aspectos (ref. def. 1.3).

Sesión de planificación de los EAA

La sesión de planificación de los EAA se lleva a cabo antes o durante la etapa 1 o antes de una auditoría posterior con aplicación de los EAA en un primer momento y después cuando se

producen cambios importantes en la organización o en el Sistema de Gestión Integrado de la organización. Las Tecnologías de la Información y la Comunicación (TIC) pueden ser utilizadas para la sesión de planificación de acuerdo con el MD4. En la sesión de planificación se examinan las siguientes aportaciones:

- Alcance de las actividades de la empresa
- Ámbito de aplicación del SGI y sus componentes
- Procesos y estructura de la organización
- Nivel de integración del SG
- Requisitos de competencia de los auditores

Se esperan los siguientes resultados:

- Confirmación de la plena integración del SG
- Confirmación de la duración de la auditoría
- Confirmar la competencia del equipo de auditoría
- Plan de auditoría

6.2. ANEXO 2 - REDUCCIÓN DEL TIEMPO DE AUDITORÍA PARA EL ENFOQUE ESTÁNDAR DE AUDITORÍA

Figure 1

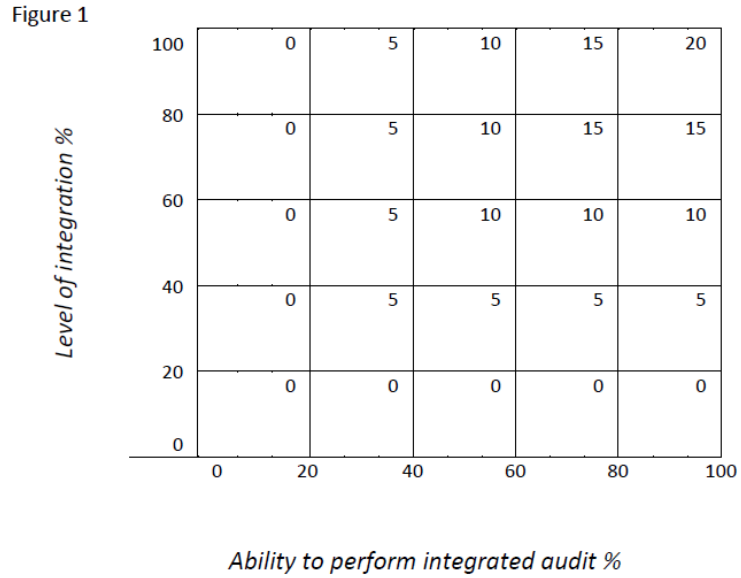


Figura 1: Esta figura ilustra la reducción (%) en la duración de la auditoría integrada y su relación con:

Eje vertical: el nivel de integración del sistema de gestión de una organización (véase más adelante), que debe incluir una consideración de la capacidad de la entidad fiscalizada para responder a preguntas multiaspecto. Un Sistema de Gestión Integrado resulta cuando una organización utiliza un único sistema de gestión para gestionar múltiples aspectos del rendimiento de la organización. Se caracteriza por (pero no se limita a):

1. Un conjunto integrado de documentación, incluyendo instrucciones de trabajo para un buen nivel de desarrollo, según corresponda;
2. Revisiones de la gerencia que consideran la estrategia y el plan general de negocios;
3. Un enfoque integrado de las auditorías internas;
4. Un enfoque integrado de la política y los objetivos;
5. Un enfoque integrado de los procesos de los sistemas;

6. Un enfoque integrado de los mecanismos de mejora (acciones correctivas y preventivas; medición y mejora continua); y
7. Apoyo y responsabilidades de la gestión integrada.

Eje horizontal: El grado, dado como una proporción que se multiplicará por 100 para alcanzar el grado en el que los miembros individuales del equipo de auditoría están calificados:

$$\frac{100\ ((X1-1) + (X2-1) + (X3-1) + (Xn-1))}{Z(Y-1)}$$

Donde
X1, 2, 3...n es el número de normas para las que un auditor está cualificado y es relevante para el alcance de la auditoría integrada;
Y es el número de normas de sistemas de gestión que deben ser cubiertas por la auditoría integrada;
Z es el número de auditores.

Ejemplo:
Un equipo de auditoría integrado por tres auditores que abarca tres normas de sistemas de gestión diferentes. Un auditor está calificado para las tres normas; un auditor está calificado para dos de las normas y el otro auditor está calificado para una norma.
El porcentaje que se utilizará para el eje horizontal es:

$$\frac{100\ ((3-1) + (2-1) + (1-1))}{3(3-1)} = 50\ \%$$

Debido a la competencia disponible de cada auditor para más de un conjunto de criterios/normas de auditoría, se obtienen eficiencias que se incluyen en el cálculo de la posible reducción de tiempo en la fórmula anterior. Estos incluyen:

1. Ahorro de tiempo gracias a una reunión de apertura y otra de clausura;
2. Ahorro de tiempo gracias a la elaboración de un informe de auditoría integrado;
3. Ahorro de tiempo en la optimización de la logística;
4. Ahorro de tiempo en las reuniones del equipo de auditores; y
5. Ahorro de tiempo al auditar elementos comunes simultáneamente, por ejemplo, control de documentos.

ANEXO I

LINEAMIENTOS DE AUDITORÍA DE CUMPLIMIENTO LEGAL PARA ISO 45001

1. INTRODUCCIÓN

1.1. Considerando los diversos puntos de vista, la siguiente definición de "cumplimiento legal"se utiliza: "Conformidad con la ley, de tal manera que se realice el resultado deseado".Si bien la certificación de un SGSST contra los requisitos de los SGSST aplicablesla norma no es una garantía de cumplimiento legal (tampoco lo es ningún otro medio de control,incluyendo el gobierno u otro tipo de control y / o inspecciones de cumplimiento legal ootras formas de certificación o verificación), es una herramienta probada y eficiente para lograr ymantener tal cumplimiento legal.Se reconoce que la certificación acreditada de SGSST deberá demostrar que un tercero independiente (organismo de certificación) ha evaluado y confirmado que La organización cuenta con un SGSST demostrablemente eficaz para garantizar el cumplimiento de su política.compromisos incluyendo cumplimiento legal.El incumplimiento continuo o potencial de los requisitos legales aplicables podríamostrar una falta de control de gestión dentro de la organización y su SGSST y elLa conformidad con la norma debe revisarse cuidadosamente.

2. PARTES INTERESADAS EN UN SGSST ISO 45001:2018

DEFINICIÓN DE PARTE INTERESADAISO 45001:2018: 3.2 parte interesada persona u organización (3.1) que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad

Se consideran por parte del equipo auditor de PERU CERTIFICACIÓN como partes interesadas de un SGSST ISO 45001:2018 y se deberá validar dentro del alcance del sistema de gestión el cumplimiento de los requisitos exigidos para evitar afectar el cumplimiento de los objetivos del SGSTT, al igual que la satisfacción percibida por la gestión del SGSTT (Cuando aplique):

1. **Autoridades legales y reguladoras (locales, regionales, nacionales o internacionales)**
2. **Organizaciones matrices**
3. **Proveedores**
4. **Contratistas y subcontratistas**
5. **Organizaciones de trabajadores (sindicatos)**
6. **Organizaciones de empleadores propietarios**
7. **Accionistas**
8. **Clientes**
9. **Visitantes**
10. **Familiares de los trabajadores**
11. **Comunidad local**
12. **Vecinos de la organización**
13. **Público en general**
14. **Servicios médicos y otros servicios comunitarios**
15. **Medios de comunicación**
16. **Academia**
17. **Asociaciones comerciales**
18. **Organizaciones no gubernamentales (ONG)**
19. **Organizaciones de seguridad y salud en el trabajo**
20. **Profesionales de la salud y la seguridad en el trabajo (por ejemplo, médicos y enfermeras).**

3. CÓMO DEBE UN ORGANISMO DE CERTIFICACIÓN AUDITAR UN SGSST CON RESPETO AL CUMPLIMIENTO LEGAL.

3.1. A través del proceso de evaluación de la certificación, un organismo de certificación debe evaluar La conformidad de una organización con los requisitos de un estándar de SGSST, ya que se relacionan con el cumplimiento legal y no otorgarán la certificación hasta la conformidad con estos requisitos pueden ser demostrados.Después de la certificación, las auditorías de vigilancia y reevaluación

posteriores realizadas por El organismo de certificación deberá ser coherente con la metodología de auditoría anterior.

3.2. Con respecto al equilibrio entre la revisión de documentos y registros y laevaluación de la implementación de SGSST durante las actividades operativas (por ejemplo, recorrido por instalaciones y otros sitios de trabajo), el Organismo de Certificación se asegurará de que se lleva a cabo una auditoría de la efectividad del SGSST.

3.3. No existe una fórmula para definir cuáles deberían ser las proporciones relativas, ya que la situación es diferente en cada organización. Sin embargo, hay algunas indicaciones de que también gran parte del tiempo de auditoría dedicado a una revisión basada en la oficina es un problema que ocurre con cierta frecuencia. Esto podría conducir a una evaluación inadecuada de la efectividad del SGSST con respecto a cuestiones de cumplimiento legal, y potencialmente se pasa por alto el bajo rendimiento, lo que lleva a una pérdida de confianza de las partes interesadas en el proceso de certificación. El organismo de certificación deberá, a través de un programa de vigilancia apropiado, asegurar queLa conformidad se mantiene durante el ciclo de certificación, normalmente tres años. Los auditores del Organismo de Certificación deberán verificar la gestión del cumplimiento legal basado en la implementación demostrada del sistema y no depender solo de resultados previstos.

3.4. Cualquier organización que no demuestre su compromiso inicial o continuo cumplimiento legal, no se certificará ni se continuará certificando como cumplimiento de requisitos de un estándar de SGSST por parte del organismo de certificación.

3.5. El incumplimiento deliberado o consistente se considerará un incumplimiento grave. Apoyar el compromiso de la política para lograr el cumplimiento legal y evitará certificación o hacer que se suspenda un certificado estándar de SGSST existente, o retirado.

3.6. Si las instalaciones y áreas de trabajo están sujetas a cierre, los riesgos de SGSST cambian, como puede que ya no existan los mismos riesgos para los empleados, pero puede haber nuevos riesgos aplicables a los miembros del público (por ejemplo, en caso de falta de mantenimiento adecuado y actividades de vigilancia). El organismo de certificación deberá verificar que el sistema de gestióncontinúa cumpliendo con el estándar SGSST y se implementa de manera efectiva con respecto de las instalaciones cerradas y áreas de trabajo y, si no, suspender el certificado.

4. CRITERIOS DE CUMPLIMIENTO PARA LA DECISIÓN DE CERTIFICACIÓN

4.1. Las partes interesadas y las partes interesadas de una organización que reclama conformidad con un estándar de SGSST. El valor percibido de la certificación acreditada en este campo está estrechamente relacionada con la satisfacción lograda por las partes interesadas en relación con el cumplimiento legal.

4.2. La organización debe ser capaz de demostrar que ha logrado el cumplimiento.con los requisitos legales de SGSST que le son aplicables a través de su propia evaluación de cumplimiento antes de que el organismo de certificación otorgue la certificación.

4.3. Cuando la organización no esté en cumplimiento legal, deberá poder demostrar que ha activado un plan de implementación para lograr el pleno cumplimiento dentro de una fecha declarada, respaldada por un acuerdo documentado con el regulador, donde sea posible por las diferentes condiciones nacionales. La implementación exitosa de este plan se considerará una prioridad dentro del SGSST.

4.4. Excepcionalmente, el Organismo de Certificación aún puede otorgar la certificación pero debe buscar evidencia objetiva para confirmar que el SGSST de la organización es capaz de lograr el cumplimiento requerido a través de la implementación completa del plan de implementación anterior dentro de la fecha de vencimiento, si ha abordado todos los peligros y riesgos de SGSST para los trabajadores y otras personas expuestas personal y que no hay actividades, procesos o situaciones que puedan oconducirá a una lesión grave y / o mala salud, y durante el período de transición ha implementado las acciones necesarias para asegurar que el riesgo de SGSST se reduzca y controle.

4.5. A través de los requisitos de ISO / IEC 17021-1, cláusula 9.4.8.3 a) y ellos resultados previstos se expresan explícitamente en el estándar aplicable de SGSST, el organismo de certificación se asegurará de que sus informes de auditoría contengan una declaración sobre conformidad y la efectividad del SGSST de la organización junto con un resumen de la evidencia con respecto a la capacidad del SGSST para cumplir con sus obligaciones de cumplimiento.

5. RESUMEN

5.1. La certificación acreditada del SGSST de una organización indica conformidad con los requisitos del estándar aplicable de SGSST e incluye una demostración ycompromiso efectivo de cumplir con los requisitos legales aplicables.

5.2. El control del cumplimiento legal por parte de la organización es un componente importante de la evaluación de SGSST y sigue siendo responsabilidad de la organización.

5.3. Debe destacarse que los auditores del Organismo de Certificación no son inspectores de Regulador de SST. No deben proporcionar "declaraciones" o "declaraciones" legales. Sin embargo, pueden "verificar la evaluación del cumplimiento legal" para evaluar la conformidad con el estándar aplicable de SGSST.

5.4. Certificación acreditada de un SGSST que cumple los requisitos del estándar de SST, no puede ser una garantía legal absoluta y continuo cumplimiento, pero ninguna certificación o esquema legal puede garantizar la legalidad y continua conformidad. Sin embargo, un SGSST es una herramienta comprobada y efectiva para lograr ymantener el cumplimiento legal y brinda a la alta gerencia información relevante y oportuna información sobre el estado de cumplimiento de la organización.

5.5. Un estándar de SGSST requiere el compromiso de cumplir con los requisitos legales. La organización debe ser capaz de demostrar que ha logrado cumplir con surequisitos legales aplicables a través de su propia evaluación de cumplimiento antes del Organismo de certificación que otorga la certificación.

5.6. Certificación de un SGSST que cumple los requisitos de un SGSST. La norma confirma que se ha demostrado que el SGSST son efectivos para lograr sus compromisos de política que incluyen el cumplimiento de las obligaciones de cumplimiento legal y proporciona fundamento y apoyo para el cumplimiento legal continuo de una organización.

5.7. Para mantener la confianza de las partes interesadas, el organismo de certificación se asegurará de que el sistema haya demostrado efectividad antes de otorgar, mantener o continuar la certificación.

5.8. El SGSST puede actuar como una herramienta para el diálogo entre la organización y sus reguladores de SST y forman la base para una asociación de confianza, reemplazando el histórico de relaciones adversas. Los reguladores de SST y el público deberían tener confianza en organizaciones con un certificado estándar acreditado de SGSST y ser capaz de percibirlos como capaces de gestionar de manera constante y constante se conformidad legal.