PROCESO DE CERTIFICACIÓN DE SISTEMAS DE GESTIÓN.

Elaborado por: Lic. Paula Velasco Martínez	Revisado por: Ing. Carlos M. Martín Herrera	Aprobado por: Dr. Rogelio González Achirica
Fecha: 09-2020	Fecha: 09-2020	Fecha: 09-2020
Firma:	Firma:	Firma:

1. Objetivo y alcance.

El presente procedimiento tiene como objetivo establecer, monitorear el proceso y metodologías en la planeación y realización de las auditorías para la evaluación de la conformidad de los Sistemas de Gestión con base a las Normas nacionales e internacionales aplicables a las actividades de certificación

El alcance del presente procedimiento es aplicable para las actividades de certificación, mantenimiento y conformidad de sistemas de gestión en todas las instalaciones del Organismo de Certificación OSG S.A de C.V. para la certificación de los Sistemas de Gestión definidos a continuación:

Certificación de Sistemas de Gestión de la Seguridad para la Cadena de Suministro
Certificación de Sistemas de Gestión Antisoborno.
Certificación de Sistemas de Gestión de la Inocuidad de los Alimentos
Certificación de Sistemas de Gestión de Seguridad de la Información
Certificación de Sistemas de Gestión de Continuidad de Negocios

Este documento establece los requisitos y el procedimiento para la certificación de la conformidad con lo establecido en las Normas nacionales e internacionales relacionadas, así como las directrices establecidas por las entidades de acreditación y los organismos internacionales y/o regionales (IAAC, ILAC e IAF).

2. Documentos de referencia.

- ✓ Ley de Infraestructura de la Calidad.
- ✓ Reglamento de la Ley Federal sobre Metrología y Normalización.
- ✓ **NMX-EC-17021-1-IMNC-2016 / ISO/IEC 17021-1:2015** Evaluación de la conformidad - Requisitos para los organismos que realizan la auditoría y la certificación de los sistemas de gestión -Parte 1: Requisitos.
- ✓ **ISO 28000:2007** Sistema de Gestión de seguridad para la cadena de suministro.
- ✓ **ISO 37001:2016** Sistemas de gestión antisoborno-Requisitos con orientación para su uso. Sistemas de gestión antisoborno-Requisitos con orientación para su uso.
- ✓ **ISO/IEC 27001:2013** Information technology - Security techniques - Information security management systems – Requirements
- ✓ **ISO 22301:2019** Security and resilience -- Business continuity management systems --- Requirements
- ✓ **ISO 22000:2018** Food safety management systems — Requirements for any organization in the food chain.
- ✓ **ISO/IEC TS 17021-9** Evaluación de la conformidad- Requisitos para los organismos que realizan la auditoría y la certificación de sistemas de gestión- Parte 9: Requisitos de competencia para la auditoría y la certificación de sistemas de gestión antisoborno.
- ✓ **ISO 19011:2018** Directrices para la auditoría de los sistemas de gestión.
- ✓ **ISO 28003:2007** Security management systems for the supply chain—Requirements for bodies providing audit and certification of supply chain security management systems.

- ✓ **ISO/IEC 27006:2015** Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
- ✓ **ISO/IEC 27006:2015 Enmienda 1 2020-03** Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems.
- ✓ **ISO/IEC 27002: 2013** Information Technology — Security Techniques — Code Of Practice For Information Security Controls.
- ✓ **ISO/IEC 27005: 2018** Information Technology — Security Techniques — Information Security Risk Management.
- ✓ **ISO/IEC 27007:2020** Information Security, Cybersecurity And Privacy Protection — Guidelines For Information Security Management Systems Auditing.
- ✓ **ISO/IEC 27008:2019** Information Technology — Security Techniques — Guidelines For The Assessment Of Information Security Controls.
- ✓ **ISO/IEC TS 17021-6:2014** Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 6: Competence requirements for auditing and certification of business continuity management systems
- ✓ **ISO** 22313**:2020** Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ✓ **ISO/TS 22003:2013** Food safety management systems.- Requeriments for bodies providing audit and certification of food safety management systems
- ✓ **NOM-251-SSA1-2009** Prácticas de higiene para el proceso de alimentos, bebidas o suplementos alimenticios
- ✓ **IAF MD 1:2018** Certificación de multisitios basados en el muestreo.
- ✓ **IAF MD 2: 2017** Transferencia de las certificaciones acreditadas de los sistemas de gestión.
- ✓ **IAF MD 3:2008** Procedimientos de vigilancias y recertificación avanzados.
- ✓ **IAF MD 4:2008** Uso de técnicas de auditoría asistida por computadora para la certificación de sistemas de gestión acreditados (CAAT).
- ✓ **IAF MD 5:2019** Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems
- ✓ **IAF MD 7:2010** Armonización de las sanciones aplicables a los organismos de evaluación de la conformidad.
- ✓ **IAF MD 10:2013** Evaluación de la competencia del Organismo de Certificación de acuerdo con la ISO/IEC 17021
- ✓ **IAF MD 11:2019** IAF Mandatory Document for the Application of ISO/IEC 17021-1 for Audits of Integrated Management Systems (Aplicable a partir del 17 de enero de 2021)
- ✓ **IAF MD 12:2016** Evaluación de Actividades de Certificación para Acreditación Transfrontera.
- ✓ **IAF MD 13:2015** Knowledge Requirements for Accreditation Body Personnel for Information Security Management Systems (ISO/IEC 27001)
- ✓ **IAF MD16:2015** Application of ISO/IEC 17011 for the Accreditation of Food Safety Management Systems (FSMS) Certification Bodies
- ✓ **PG-OSG 01** Control de Documentos.
- ✓ **PG-OSG 02** Control de Registros.
- ✓ **P-OSG 01/20** Disposiciones del Presidente.
- ✓ **R-OSG** Reglamento de Certificación.
- ✓ **P-OSG 03/20** Tarifas Públicas de Certificación y Formas de Pago.
- ✓ **PG-OSG 04** Auditoría interna.
- ✓ **PE-OSG 17** Auditorias a Distancia

3. Definiciones.

Certificación de Sistemas de Gestión: Se refiere al proceso de evaluación del Sistema de Gestión del Cliente verificado que se encuentre correctamente implementado bajo la norma solicitada.

Auditoría Etapa 1: Auditoría para revisión documental y en sitio, donde se comprueba el grado de implementación del Sistema de Gestión previo a la auditoría de Etapa 2, esta es aplicable en auditorías de certificación inicial y en caso de requerirse durante las auditorías de recertificación.

Auditoría Etapa 2 o de certificación: Auditoría en sitio, donde se evalúa la implementación, incluyendo la eficacia del Sistema de Gestión del Cliente.

Auditoría de vigilancia: Auditoría en sitio realizada de forma anual en el 1er y 2^{o} año con el fin de que el Organismo de Certificación realice seguimiento al cumplimiento de los requisitos de la norma a través de las áreas y funciones representativas cubiertas por el alcance del Sistema de Gestión.

Auditoría de recertificación: Auditoría en sitio que se realiza en un periodo al término del ciclo de la certificación para la renovación de la certificación de la misma, donde se revisa nuevamente la implementación del Sistema de Gestión de manera completa cuando aplica y puede tener Etapa 1 y Etapa 2.

Auditoría de restauración: Auditoría en sitio la cual el Organismo de Certificación puede restaurar la certificación dentro los 6 meses siguientes al vencimiento de su certificación inicial. La restauración se puede llevar a cabo siempre y cuando se hayan completado las actividades de recertificación pendientes; en caso contrario de debe realizar una Etapa 2. La vigencia del certificado deberá ser la fecha de decisión de la nueva certificación o una posterior, manteniendo la fecha de expiración del ciclo del certificado anterior

Auditorías de seguimiento: Auditorías extraordinarias programadas en sitio y en algunos casos de forma remota para comprobar la implementación y efectividad de las acciones correctivas establecidas por el Cliente para solventar las no conformidades detectadas en alguna Etapa de auditoría.

Auditorías Especiales: Incluyen auditorías con notificación a corto plazo para verificar que los cambios efectuados en el Sistema de Gestión continúan cumpliendo con la norma de referencia para la certificación, seguimiento a reclamaciones o quejas presentadas por la autoridad y/o por alguna parte interesada.

Auditoría combinada: Auditoría llevada a cabo a un único auditado en dos o más sistemas de gestión.

Auditoría conjunta: Auditoría llevada a cabo a un único auditado por dos o más organizaciones auditoras.

Ampliación al alcance de la certificación: Adición de alcance o procesos, o cuando se amplíen las actividades o emplazamientos objeto de la certificación.

Reducción al alcance de la certificación: Exclusión de las partes del alcance de la certificación que no cumplen los requisitos; cuando el Cliente ha dejado de cumplir en forma persistente o grave los requisitos de la certificación. Dicha reducción está alineada con los requisitos de la norma utilizada para la certificación.

Transferencia de la certificación: La transferencia de la certificación se define como el reconocimiento de una certificación del Sistema de Gestión existente y válido, otorgado por un Organismo de Certificación acreditado, (en adelante el " Organismo de Certificación emisor"), por otro Organismo de Certificación acreditado, (en adelante el " Organismo de Certificación que acepta") con el fin de emitir su propia certificación.

Instalación principal o sede: Domicilio en donde se realizan las principales actividades de la organización,

Auditoría de Transferencia: Cuando el Cliente solicita la transferencia de su certificado vigente otorgado por otro organismo, para que sea certificado por OSG, en seguimiento a lo establecido en el documento mandatorio IAF MD 2.

Multisitio. Cuando la empresa a auditar cuenta con dos o más domicilios fijos donde se realizan actividades similares a la de la instalación principal o sede.

Sitio temporal. Domicilio de la empresa a auditar donde se realizan actividades en otras instalaciones por tiempo determinado.

Hallazgo de Auditoría: Resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría, se puede indicar Conformidad, No Conformidad Mayor, No Conformidad Menor, Oportunidad de Mejora y/o Observaciones y No Conformidad (En el caso de Etapa 1).

No Conformidad Mayor: Incumplimiento de un requisito que afecta a la capacidad del Sistema de Gestión para lograr los resultados previstos. Las no conformidades pueden ser clasificadas como mayores 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.

No Conformidad Menor: Incumplimiento de un requisito que no afecta la capacidad del Sistema de Gestión para lograr los resultados previstos. 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.

Oportunidad de Mejora y/o Observaciones: Oportunidades de mejora relacionadas con las áreas o procesos de la organización que cumplen con los requisitos mínimos del estándar, pero que pueden ser desarrollados. Es una declaración de que puede existir mayor control en algún proceso, las oportunidades de mejora deberán ser atendidas, en caso que no lo sean podrá subir a una no conformidad menor.

No conformidades: Incumplimiento parcial de requisitos que no afectan directamente al producto, solo se aplica en ETAPA 1.

4. Responsabilidades.

- ✓ La máxima responsabilidad por el cumplimiento de este procedimiento recae en la Secretaría Ejecutiva de OSG, Implantando el presente procedimiento y controlando su adecuada ejecución, revisa y propone los cambios, mejora o derogación de la documentación a la Secretaría Técnica de los documentos que no cumplen con el propósito que fueron elaborados.
- ✓ Secretaría Técnica debe de asegurarse de la Implantación y distribución del presente procedimiento, controlando su adecuada ejecución, revisa y propone los cambios, mejora o derogación de esta documentación al Presidente.
- ✓ La Secretaría Ejecutiva Iniciará el Expediente de Certificación cuando se acepte la Solicitud Certificación, Incluirá toda la documentación que se genere durante el proceso de certificación.
- ✓ La Secretaría Ejecutiva asentará en el Registro RPE-OSG 01.2 Registro Solicitud de Certificación las solicitudes de certificación y le asignará el número que lo identifica, el cual coincide con el No. de Expediente de Certificación.

5. Generalidades del proceso de certificación.

5.1 Solicitud de certificación.

La Secretaría Ejecutiva recibe el **RPE-OSG 01.1** Solicitud de Certificación de Sistemas de Gestión vía correo electrónico o en físico, mediante documento impreso o digital por parte del solicitante, la cual deberá incluir lo necesario referente a la información del sistema del Cliente bajo la norma solicitada, la Secretaría Ejecutiva será la encargada de dar seguimiento a dicha solicitud a fin de asegurarse de lo siguiente:

a) La información de la organización solicitante y su Sistema de Gestión cumple con los requisitos para realizar Etapa 1 y el Programa.
b) Cualquier diferencia ha sido resuelta entre el Organismo de Certificación y la organización solicitante.
c) El Organismo de Certificación tiene la competencia y la capacidad para llevar a cabo la actividad de certificación. Revisando el alcance de la organización y la competencia de nuestros auditores.
d) Se tienen en cuenta el alcance de la certificación solicitada, las ubicaciones donde la organización solicitante lleva a cabo sus operaciones, 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.).
e) Firmar el contrato correspondiente, en el cual se establecerán los compromisos relacionados con los deberes, derechos y responsabilidades de ambas partes.
f) Comprobante de pago por servicios de certificación. El costo de la certificación se considerará en base a las Tarifas Públicas del Servicio de Certificación y las Formas de Pago, establecidas en la Disposición D-OSG 03/20.

La presentación de la solicitud deberá ser preferentemente presencial, con la participación de la persona designada por la organización, con los conocimientos de los elementos necesarios del Sistema de Gestión a certificar a fin de evacuar en el momento las posibles dudas o corregir errores.

La solicitud será revisada en conjunto con la Secretaría Técnica y registrada por la Secretaría Ejecutiva en el registro **RPE- OSG 01.2** Registro Solicitud de Certificación, para verificar que los datos que se encuentren en ella sean apropiados para realizar la Etapa 1, Programa de Auditoría, la programación y se verificara que los días auditor sean los correctos. La selección del Equipo Auditor será realizada por la Secretaría Ejecutiva.

La revisión de la solicitud deberá considerar:

a) Datos de la organización solicitante:
- ✓ Nombre de la empresa.
- ✓ Nombre del contacto.
- ✓ Norma a certificar.
- ✓ Número de personal.

b) Datos del sistema:
- ✓ Implementación de Sistema de Gestión según la norma solicitada.
- ✓ Alcance.
- ✓ Grado de Integración (cuando aplique).

c) Datos de direcciones:
- ✓ Sede, Sitio, Multisitio y/o sitio temporal.

En caso de faltar alguno, la Secretaría Ejecutiva será responsable de contactar al Cliente para recabar los requisitos; si el Cliente envía la información complementaria o corregida, continúa con el proceso de revisión, si no se recibe la información en un plazo máximo de 10 días hábiles se cancela la solicitud y se documenta la causa por la cual se cancela por medio de un correo electrónico.

El Cliente tiene libre acceso para formular su interés ante OSG, y puede solicitar que se le envíe una oferta preliminar de cotización del servicio de certificación contenida en el **Anexo A de la Disposición D-OSG 03**, cuyo cálculo se hará en base a la información suministrada por la Organización Cliente en la Solicitud de Certificación ingresada de acuerdo al alcance requerido **RPE-OSG 01.1** Solicitud de Certificación de Sistemas de Gestión dicho formato se encuentra disponible en el sitio web.http://osgorganismodecertificacion.mx la que estará sujeta a la aprobación por el Cliente,

La Secretaría Ejecutiva deberá demostrar el proceso de investigación seguido, cómo éste ha sido registrado como parte de las auditorías de Etapa 1 y Etapa 2 y como es empleado por el personal relevante que realiza las actividades de certificación (ISO 17021-1 Anexo 1). Para garantizar la coherencia, se prevé que la Evaluación de la Conformidad (EC) necesite un procedimiento documentado que describa la forma en que se realiza esta investigación independiente.

Una vez recibidos los documentos completos la Secretaría Ejecutiva elabora el Expediente de Certificación para poder realizar la Etapa 1, asignando la referencia correspondiente, la cual se asigna de la siguiente manera:

a) Número consecutivo del Cliente XX
b) Año de ingreso de la solicitud: AA

Para los Clientes iniciales el número de solicitud coincide con el número del Expediente de Certificación, para los Clientes continuantes mantienen el número de su registro inicial excepto cuando se proceda a la recertificación donde se confecciona un nuevo expediente, manteniendo los documentos anteriores dentro de este.

Consideraciones adicionales por alcance de certificación.

Certificación Antisoborno.

Para el alcance de certificación antisoborno, si bien se reconoce que una auditoría del Sistema de Gestión ISO 37001 no implica una investigación en profundidad del Cliente, la Secretaría Ejecutiva debería realizar una investigación de antecedentes a través de Internet (es decir, herramientas y técnicas de investigación de fuentes abiertas) o de información pública disponible en cada uno de los países, por ejemplo, para asegurarse de que el Cliente no implica riesgos adicionales como consecuencia de acusaciones/casos de soborno pendientes o informes adversos en los medios de comunicación los cuales no haya declarado. Una simple revisión de la información proporcionada por el Cliente y de los detalles ofrecidos en su web es improbable que resulte suficiente.

Para el alcance de certificación antisoborno OSG realizará un diagnóstico previo para valorar la comprensión de la organización (Cliente) y de su contexto con el objetivo de determinar las cuestiones internas y externas que son pertinentes para su propósito y que afectan su capacidad para lograr los objetivos previstos de su Sistema de Gestión Antisoborno, este diagnóstico previo tiene en cuenta los requisitos establecidos en el apartado No 4 de la norma.

Para certificación del sistema de gestión antisoborno, si la organización cliente solicita la exclusión de ubicaciones geográficas o actividades concretas (por ejemplo, actividades distintas a ventas, operaciones, proveedores, socios comerciales y mercados existentes), Secretaria Ejecutiva deberá confirmar que estas exclusiones no presentan riesgos de soborno que podrían socavar el alcance y el funcionamiento del sistema de gestión anti- soborno. Si se pretenden excluir áreas clave, se debería solicitar una justificación para ofrecer tal certificación.

Certificación de seguridad de la información.

Los procedimientos de certificación se centrarán en establecer que el SGSI de un cliente cumple los requisitos especificados en ISO / IEC 27001 y las políticas y objetivos del cliente.

Como requisito para el ingreso de la solicitud del servicio de certificación, la organización debe contar con un sistema de gestión de seguridad de la información implementado de conformidad con los requisitos de la norma ISO 27001: 2013, así como sus normas aplicables, asimismo deberá proporcionar el acceso a los informes de auditoría interna e informes de revisiones independientes de la seguridad de la información.

El cliente deberá proporcionar al menos la siguiente información:

a) información general sobre el SGSI y las actividades que cubre;
b) una copia de la documentación requerida del SGSI especificada en ISO / IEC 27001 y, cuando sea necesario, la documentación asociada.

El alcance y los límites de la certificación del SGSI deberán estar claramente definidos contra todos los requisitos de certificación aplicables, considerando las características del negocio, el ámbito del SGSI de la organización, su ubicación, activos y tecnología, este deberá indicarse a través de la Declaratoria de Aplicabilidad.

Para efectos de la certificación se requiere asegurar que las interfaces con los servicios y las actividades que no están completamente dentro del alcance del SGSI sean señaladas dentro del sistema de gestión y sean incluidas dentro del análisis de riesgos de la seguridad de la información.

Los objetivos de la auditoría de un SGSI, incluirán la determinación de la efectividad del sistema de gestión para garantizar que el cliente, de acuerdo con la evaluación de riesgos, haya implementado los controles aplicables y haya alcanzado los objetivos de seguridad de la información establecidos.

Certificación de inocuidad de los alimentos.

Para la determinación del alcance se debe considerar como referencia la categorización señalada en la norma ISO 22003:2013, también se debe contemplar todas las actividades, procesos, productos o servicios que puedan influir en la inocuidad del producto final definido en el alcance de la certificación.

5.2 Programa de auditoría

Una vez creado el Expediente de Certificación se designa al auditor que cuente con la competencia necesaria para el alcance indicado en la solicitud de servicio para la elaboración del Programa de Auditoría establecido en el **RPE-OSG 01.3** Programa de Auditoría en el que se establecerán las fechas propuestas para el ciclo completo de la certificación y las Etapas 1 y 2 para las auditorías de certificación inicial y lo correspondiente en el caso de vigilancias y/o recertificaciones, donde sólo aplicará la realización de auditorías en etapa 2; tomando como base los criterios establecidos en el procedimiento **PSG-OSG 15** Determinación de Tiempo de Auditoría.

La Secretaría Ejecutiva quien en lo adelante se responsabiliza en nombre de OSG con las relaciones directas con el cliente, informa toda la planificación del servicio de certificación para conocer si existe alguna discrepancia, que debe fundamentarse documentalmente, sobre algún miembro del equipo que contravenga la transparencia o imparcialidad del proceso, así como con la propuesta de plazos para la ejecución de cada etapa. OSG establece una Visita Previa para certificaciones iniciales con el objetivo de evaluar en sitio las condiciones para el servicio incluye entrevistas, recorridos, observación visual, entre otras.

En caso que las condiciones lo ameriten o bien que sea solicitado por el cliente certificado, se puede considerar la alternativa de realizar las auditorías a distancia de acuerdo a lo establecido en el procedimiento de Auditorias a Distancia **PE-OSG 17**.

El Programa de Auditoría se elabora de acuerdo al tiempo utilizado en cada auditoría y dependerá de varios factores como el alcance del Cliente; tamaño y complejidad de la organización; contratación externa, requisitos tecnológicos y reglamentarios, resultados de auditorías anteriores, número de sitios a auditar o multisitio, la madurez de su Sistema de Gestión y lo que se conoce de sus propios procedimientos de auditoría interna.

El Programa de Auditoría debe, al menos, incluir o hacer referencia a lo siguiente:

a) los objetivos de la auditoría;
b) los criterios de la auditoría;
c) el alcance de la auditoría, incluida la identificación de las unidades organizacionales y funcionales o los procesos por auditar;
d) las fechas y los sitios en los que se van a realizar las actividades de auditoría in situ, incluidas las visitas a los sitios temporales y actividades de auditoría a distancia o remota, cuando corresponda;
e) la duración prevista para las actividades de auditoría in situ; y
f) los roles y las responsabilidades de los miembros del equipo auditor y de las personas que los acompañan, tales como observadores e intérpretes.
g) en caso de realizar auditorías a distancia de manera parcial o total, deberá indicarse en el programa, las actividades o procesos que se auditarán mediante esta técnica.

Consideraciones adicionales por alcance de certificación.

Certificación Antisoborno.

En el caso que la Organización (Cliente) solicita la exclusión de ubicaciones geográficas o actividades concretas (por ejemplo, actividades distintas a ventas, operaciones, proveedores, socios comerciales y mercados existentes), la Secretaría Ejecutiva deberá confirmar que estas exclusiones no presentan riesgos de soborno que podrían socavar el alcance y el funcionamiento del Sistema de Gestión Antisoborno. Si se pretenden excluir áreas clave, se debería solicitar una justificación para ofrecer tal certificación.

La Secretaría Ejecutiva debe explicar a sus clientes su política sobre el alcance de la certificación para que los solicitantes sean conscientes y conocedores de sus expectativas en relación al alcance de aplicación del Sistema de Gestión Antisoborno dentro de la entidad legal del Cliente.

Certificación de inocuidad de los alimentos.

En la programación de la auditoría correspondiente a la inocuidad de los alimentos se debe considerar la elección de las fechas de auditoría contemplando el tiempo, estación del año, de acuerdo al producto contemplado en el alcance a certificar; con la intención que el Equipo Auditor tenga la oportunidad de auditar a la organización operando un número representativo de líneas de producción, contemplando que las categorías o subcategorías aplicables sean cubiertas en el alcance de la certificación.

Certificación de seguridad de la información.

El Plan de Auditoría para las auditorías del SGSI deberá tener en cuenta los controles de seguridad de la información determinados.

En caso de requerirse, el Plan de Auditoría identificará las técnicas de auditoría asistidas por medios electrónicos que se utilizarán durante la auditoría, según corresponda.

Las técnicas de auditoría asistidas por medios electrónicos pueden incluir, por ejemplo, teleconferencia, reunión web, comunicaciones interactivas basadas en la web y acceso electrónico remoto a la documentación o procesos del SGSI. El enfoque de tales técnicas debe ser mejorar la efectividad y eficiencia de la auditoría y debe respaldar la integridad del proceso de auditoría.
Durante la planeación se debe acordar con la organización el momento en que se llevará a cabo la auditoría con la finalidad de demostrar la auditoría del alcance completo de la organización, esta consideración puede considerar la temporada, fechas de auditoría específicas y el/los turno(s) según se requiera.

5.2.1 Auditoría de Certificación Multisitio.

Cuando se tenga una solicitud para Certificación Multisitio se deberá proceder de acuerdo al Procedimiento de Auditorías Multisitios e Integradas **PE-OSG 16.**

5.2.2 Transferencias de Certificación.

Es la auditoría realizada por OSG para demostrar el cumplimiento de una Organización que ha requerido la transferencia de su certificado* otorgado por otro Organismo de Certificación acreditado en el mismo alcance que OSG y para lo cual se consideran las bases establecidas en el documento mandatorio IAF MD 2:2017.

La solicitud de transferencia se debe ingresar a la Secretaría Ejecutiva y una vez recibida hará la revisión de dicha solicitud para evaluar en qué etapa se localiza la organización del Cliente, tipo de normatividad aplicable, cuáles son sus necesidades y verificar que la revisión pre transferencia con base en lo establecido en el documento mandatorio IAF MD2.

La auditoría de transición deberá cubrir los siguientes aspectos como mínimo y la revisión y sus hallazgos deberán estar completamente documentados:

a) Confirmación de que la Certificación del Cliente se encuentra dentro del alcance acreditado del Organismo de Certificación emisor y aceptante;
b) Confirmación de que el alcance acreditado del Organismo de Certificación emisor se encuentra dentro del alcance de MLA de su organismo de acreditación;
c) Las razones para buscar una transferencia;
d) Que el sitio o los sitios que desean transferir la certificación posean una acreditación válida proceso de dar un título;
e) Para la certificación inicial o los informes de auditoría de recertificación más recientes, y el último informe de vigilancia; que el estado de todas las no conformidades pendientes que puede surgir de ellos y de cualquier otra documentación relevante disponible con respecto al proceso de certificación. Si estos informes de auditoría no están realizados, disponibles o si la auditoría de vigilancia o auditoría de recertificación no ha sido completada según lo requerido por el programa de auditoría del organismo emisor de la certificación, entonces la organización debe ser tratada como un nuevo Cliente;
f) Quejas recibidas, de las cuales se ha verificado la implementación de las medidas tomadas para su atención;
g) Consideraciones relevantes para establecer un plan de auditoría y una auditoría programa. El programa de auditoría establecido por la certificación emisora el cuerpo debe ser revisado si está disponible, de acuerdo a lo establecido en el documento IAF MD 2;

h) Cualquier compromiso actual del Cliente que realiza la transferencia con los organismos reguladores relevantes para el alcance de la certificación con respecto al cumplimiento legal.

Si no se cumplen con los requisitos para realizar la transferencia, se rechaza la solicitud y se notifica el motivo al Cliente. Si se acepta la solicitud, se identificará la Etapa en la que se encuentra la organización para realizar el Programa de Auditorías, para vigilancia se debe considerar evaluar:

1. Auditorías internas y la revisión por la Dirección, requisitos de la documentación, planificación, seguimiento y medición, mejora.
2. Eficacia del Sistema de Gestión y cumplimiento con los objetivos de la organización certificada.
3. Seguimiento de Quejas y/o Apelaciones.
4. Seguimiento a las acciones derivadas de las no conformidades de la auditoría anterior.
5. Mejora continua.
6. Revisión de cambios en la organización posteriores a la última visita.

En caso de que la organización sea considerada como Cliente nuevo, se realizará el plan correspondiente, si es una vigilancia o recertificación, se seguirá el programa previo.

5.3 Designación del Equipo Auditor.

Tomando como base el Programa de Auditoría la Secretaría Ejecutiva solicitará la información al Cliente, que consiste en el manual de calidad, políticas y procedimientos de acuerdo al tipo de auditoría referido en 5.4.

La Secretaría Ejecutiva designa al Equipo Auditor calificado para el alcance requerido con base en el Listado de Auditores Calificados y solicitara disponibilidad al auditor para las fechas propuestas.

Una vez confirmada su disponibilidad notificará al Cliente el tipo de auditoría a realizar, indicando la designación del Equipo Auditor y fecha de auditoría a través de la Notificación de Auditoría, misma que deberá enviarse al menos 15 días antes de la fecha de auditoría.

Una vez que se acepta el equipo y se tienen confirmadas las fechas, se puede continuar proceso de acuerdo al tipo de auditoría correspondiente. En caso de que la organización no acepte fecha o grupo, deberá solicitar por escrito el cambio de fechas para la celebración de la auditoría o de algún auditor o experto técnico, debido a posibles conflictos de intereses, como se mencionan a continuación:

a) En caso de que exista una relación Cliente-proveedor en los últimos tres años
b) Actividades de trabajo con el Cliente en los últimos tres años.
c) Falta de competencia técnica.
d) Riesgos derivados de omisiones por parte del Organismo o aquellos identificados en la Matriz de riesgos.

Se deberá presentar la evidencia que soporte el conflicto de interés declarado por el Cliente.

Para la Auditoría que corresponda, el Auditor Líder preparará el Plan de Auditoría de acuerdo a los documentos enviados por el Cliente en el registro **RPE-OSG 01.4** Plan de Auditoría. El auditor Líder asigna las funciones al Equipo Auditor dependiendo la complejidad del sistema, normas a auditar y conocimientos técnicos, para llevar a cabo la auditoría, con base en la información necesaria del Sistema de Gestión de la Organización a auditar proporcionada por el Organismo de Certificación, elabora y se envía a la Secretaría Técnica para su aprobación a más tardar con 10 días antes de la fecha de auditoría, para que se esté informado de las actividades.

En caso de que el auditor necesite más información del Cliente, se solicitara a la Secretará Ejecutiva.

La Secretaría Técnica en consulta con la Secretaría Ejecutiva considerará la necesidad de incluir experto(s) técnico(s), auditor en entrenamiento y/u observadores previo consentimiento del Cliente, la Secretaría Ejecutiva junto con el Cliente, determinará la fecha para la realización de la auditoría y los arreglos necesarios para aceptar y recibir al personal antes descrito. Todo el personal asistente a una auditoría, incluyendo su función, deberá estar indicado en la notificación correspondiente contenida en el Plan de Auditoría.

La Secretaría Técnica confirma el contenido del Plan de Auditoría a través de su revisión y aprobación mediante nombre y firma y se entrega al Auditor Líder para que sea enviado al Cliente. Este deberá ser enviado al menos 3 días antes de la realización de la auditoría.

Consideraciones adicionales por alcance de certificación.

Certificación Antisoborno.

Los criterios de competencia se determinarán con respecto a los requisitos de la norma del Sistema de Gestión Antisoborno, para cada área técnica y para cada función en el proceso de certificación. Los requisitos específicos de competencia en relación a la gestión antisoborno, se han establecido el procedimiento **PE-OSG 02** Criterios de Competencia.

De acuerdo a la norma ISO/IEC TS 17021-9 se requiere que el Equipo Auditor tenga conocimiento práctico y una comprensión tanto de cómo se manifiesta el soborno en el sector de negocio específico y la ubicación geográfica del Cliente como de los canales y mecanismos por los que se lleva a cabo el mismo; del contexto y del sector de negocio de la Organización Cliente; diseño y evaluación de controles antisoborno; conocimiento respecto a los riesgos de soborno pertinentes a las actividades de negocio de la organización cliente y que pueda emitir juicios respecto a la evaluación de dichos riesgos; conocimiento de la legislación aplicable en la materia, de acuerdo a los países, regiones o mercados donde se desarrollan las actividades del negocio.

Para lo anterior, OSG considera la formación de auditores de otros Sistemas de Gestión para esta certificación, para lo cual el Equipo Auditor adquiere el conocimiento práctico y la comprensión de los riesgos de soborno y de los controles que deberían ser adecuados según el sector y área geográfica en que sean evaluados como competentes para auditar, además de conocer los conceptos de Sistema de Gestión Antisoborno y los requisitos de ISO 37001.

Certificación de seguridad de la información.

Un equipo de auditoría puede estar formado por una persona, siempre que cumpla con todos los criterios de competencia establecidos en el procedimiento **PE-OSG 02** Criterios de Competencia, así como en el alcance de la certificación.

Para actividades de vigilancia y auditoría especial, se aplican los requisitos que son relevantes para la actividad de vigilancia programada y la actividad de auditoría especial.

Al seleccionar y administrar el equipo de auditoría que se designará para una auditoría de certificación específica, OSG garantizará que las competencias aportadas a cada tarea sean apropiadas.

El equipo deberá:

a) tener conocimiento técnico apropiado de las actividades específicas dentro del alcance de la certificación del SGSI y, cuando corresponda, el conocimiento relacionado con los procedimientos asociados y los riesgos potenciales de seguridad de la información (dicha actividad puede ser cubierta por el experto técnico designado);
b) tener una comprensión del cliente suficiente para realizar una auditoría de certificación confiable de su SGSI dado el alcance y el contexto del SGSI dentro de la organización;
c) tener una comprensión adecuada de los requisitos legales y reglamentarios aplicables al SGSI, esto no implica conocimientos profundos en materia legal.

5.4 Tipos de Auditoría.

En esta Etapa se describen los tipos de auditoría dependiendo del proceso, considerando a realizar:

- Auditoría Etapa 1 ver apartado 5.4.1
- Auditoría Etapa 2 ver apartado 5.4.2
- Auditoría de Vigilancia ver apartado 5.4.3
- Auditoría de Recertificación ver apartado ver apartado 5.4.4
- Auditorías especiales (ampliación de alcance, con notificación a corto plazo) ver apartado 5.4.5

5.4.1 Auditoría Etapa 1

Los objetivos de la Auditoría Etapa 1 son:

a) Evaluar la documentación del Sistema de Gestión de la Organización (Procedimientos de Gestión).
b) Evaluar las condiciones de la ubicación y los sitios específicos de la Organización y llegar a acuerdos con el personal de la Organización para determinar el grado de preparación de la Organización para la realización de la auditoría Etapa 2.
c) Revisar el estado del Cliente y su entendimiento de los requisitos de la norma, particularmente lo relativo a la identificación del desempeño clave o aspectos, procesos u objetivos relevantes y la operación del SG a través de la revisión documental.

d) Recolectar la información necesaria respecto al alcance de la certificación, los procesos y equipos empleados, y sitios de la Organización niveles de controles establecidos y los aspectos legales y/o reglamentarios y jurídicos relacionados y su cumplimiento.
e) Revisar la asignación de los recursos y acordar con la Organización los detalles para la auditoría Etapa 2.
f) Definir un enfoque preciso para la planificación de la auditoría de Etapa 2 a través de obtener un entendimiento suficiente del SG de la Organización del Cliente y de las operaciones del sitio en el contexto de posibles aspectos significativos.
g) Evaluar si las Auditorías Internas y la Revisión por la Dirección de la Organización han sido planificadas y llevadas a cabo y si el nivel de implantación del SG ofrece una confianza adecuada de que la Organización está lista para la auditoría de Etapa 2.
h) Política de seguridad en cadena de suministro.
i) Determinación de riesgos y oportunidades de acuerdo al Sistema de Gestión solicitado.
j) Identificación de peligros y valoración de riesgo.
k) Resultado de la última Revisión por la Dirección.
l) Resultado de la última Auditoría Interna.

La Secretaría Ejecutiva turnará a un Auditor Líder calificado la información documental entregada por el Cliente, e iniciará la programación de la Etapa 1, la cual dependiendo el alcance, contexto y condiciones de la Organización podrá realizarse de manera documental o en las instalaciones del Cliente, concluida dicha evaluación se emite en el **RPE-OSG 01.5** Informe Auditoría Etapa 1 el cual debe indicar si la documentación presentada es aceptable o en su caso mencionar los hallazgos detectados, los cuales deberán ser tratadas por el Cliente antes de la Etapa 2, presentando a Secretaría Ejecutiva por el Cliente el registro **RPE-OSG 01.6** Informe Cierre de Acciones Correctivas, en un término de treinta (30) días naturales a partir de la entrega del informe, ya que estos hallazgos se revisarán durante la visita. El Auditor Líder cuenta con cinco (5) días naturales para entregar el Informe a la Secretaría Técnica para su revisión, esta a su vez cuenta con tres (3) días naturales para su entrega a la Secretaría Ejecutiva quien contará con dos (2) días naturales para su entrega al Cliente.

En caso de no ser atendidos se integrarán nuevamente al Informe Final de la conclusión de la Auditoría Etapa 2 considerándose como No Conformidad Mayor. El informe deberá ser entregado por parte del auditor a la Secretaría Ejecutiva, la cual antes de enviarlo al Cliente debe ser revisado por parte de la Secretaría Técnica dejando constancia de su revisión en el registro **RPE OSG 01.7** Revisión Técnica. La Secretaría Ejecutiva entrega al Cliente los resultados documentados por la Secretaría Técnica, que resumen los resultados y conclusiones de la Etapa 1, para pasar a la Etapa 2, es necesario presentar el cierre de los hallazgos de la Etapa 1 presentados por el Cliente en el Informe Cierre de Acciones Correctivas.

Al determinar el intervalo entre la Etapa 1 y la Etapa 2, se deben considerar las necesidades del Cliente para resolver los hallazgos en la Etapa 1. El Organismo de Certificación revisará los acuerdos para la Etapa 2. Si ocurren cambios significativos que pudieran impactar el Sistema de Gestión, el Organismo de Certificación debe considerar la necesidad de repetir toda la Etapa 1, o una parte de ella.

La Secretaría Ejecutiva deberá informar al Cliente cuando los resultados de la Etapa 1 puedan conducir al aplazamiento o cancelación de la Etapa 2.

El intervalo entre Etapa 1 y Etapa 2 no debe exceder los dos (2) meses, ni inferior a treinta (30) días naturales entre las Etapas 1 y 2 para la solución por el Cliente si procede de los hallazgos que comprometen la conformidad con los requisitos establecidos.
De no solucionarse en el plazo reglamentado debe analizarse por Secretaría Ejecutiva las causas y la toma de decisión correspondiente por el incumplimiento de este requisito a causa de la extemporaneidad de los resultados auditados. Cuando el período entre la Etapa 1 y 2 pasa de los tres (3) meses se repite la Etapa 1.

Una vez que se haya decidido continuar el proceso de certificación de la conformidad, el auditor líder elaborará el plan de la auditoria, que precisa las actividades a realizar in situ y sus fechas de ejecución, esta información es remitida al cliente a través de la Secretaría Ejecutiva para su puntualización y aprobación por ambas partes, una vez aprobado el plan de auditoría este no puede ser modificado y en caso de algún cambio se puntualiza en la reunión de apertura y se deja constancia escrita de los cambios previo acuerdo de las partes.

Consideraciones adicionales por alcance de certificación.

Certificación Antisoborno.

En relación al Sistema de Gestión Antisoborno, para avanzar desde la Etapa 1 a la Etapa 2, se espera que el Equipo Auditor confirme que el Cliente ha identificado y documentado los riesgos de soborno que podría razonablemente anticipar (ISO 37001 cláusula 4.5.1) y que la Organización ha definido las medidas de control antisoborno relevantes para su modelo de negocio, entorno operativo y relaciones externas e internas, incluidos los acuerdos de la cadena de suministro.

El Equipo Auditor deberá asegurarse de que el Cliente haya identificado a todos los socios comerciales (según se define en ISO 37001, cláusula 3.26) y el riesgo de soborno al que pueden al Cliente.

El Equipo Auditor deberá determinar las ubicaciones que deben auditarse para asegurar la evaluación de la implementación efectiva del Sistema de Gestión Antisoborno. Los factores a considerar podrían incluir el nivel de riesgo de país, los sectores de mayor riesgo, las jurisdicciones y la gestión y el rol de los socios comerciales.

Las actividades subcontratadas no se incluirán directamente en el alcance de la auditoría, pero (como ocurre con ISO 9001) la gestión de las actividades subcontratadas deberá incluirse en los procesos generales de auditoría.

Se prevé que la evaluación del Cliente de su riesgo de soborno y los factores anteriormente indicados, aporten información al Equipo Auditor para la planificación y determinación de la duración de la auditoría de Etapa 2 (ISO 17021-1, cláusula 9.1.4.2.g).

Certificación de inocuidad de los alimentos.

Los objetivos de la Etapa 1 son proporcionar un enfoque para la planificación de la auditoría de la Etapa 2 mediante la comprensión del SGIA de la Organización y el estado de preparación de la Organización para la Etapa 2, analizando en qué medida:

a) Ha identificado la organización los prerrequisitos (PRP´s) que son apropiados para el negocio.
b) El SGIA incluye los procesos y métodos adecuados para la identificación y evaluación de los peligros para la inocuidad de los alimentos de la Organización, y la subsiguiente selección y categorización de las medidas de control.
c) La legislación sobre inocuidad de los alimentos para el o los sectores pertinentes de la Organización.
d) El SGIA está diseñado para lograr la política de inocuidad de los alimentos de la Organización.
e) El programa de implementación del SGIA justifica la realización de la auditoría (Etapa 2).
f) Los programas de validación, verificación y mejora cumplen los requisitos de la norma de SGIA.
g) Los documentos y acuerdos sobre el SGIA están en el sitio para comunicarlos internamente y a los proveedores, clientes y partes interesadas pertinentes, y
h) Hay que revisar la documentación adicional y/o qué conocimientos hay que obtener con anticipación.

En caso que una Organización haya implementado una combinación de medidas de control desarrollada externamente, la Etapa 1 deberá revisar la documentación incluida en el SGIA para determinar si la combinación de medidas de control:

- es adecuado para la organización,
- fue desarrollado de conformidad con los requisitos de ISO 22000, y
- se mantiene actualizado.

La disponibilidad de las autorizaciones relevantes se verificará al recopilar la información sobre el cumplimiento de los aspectos reglamentarios.

Para un SGIA, la auditoría de la Etapa 1 debe realizarse en las instalaciones del cliente con el fin de lograr los objetivos indicados anteriormente, en casos excepcionales parte de la Etapa 1 puede realizarse de manera documental lo cual deberá justificarse. La evidencia de cumplimiento de la Etapa 1 deben ser provistos por la Organización y en casos excepcionales se puede incluir la revisión de sitios remotos o de producción estacional.

Cualquier parte del SGIA que sea auditado durante la Etapa 1 de manera completa, que se determine durante dicha etapa que se encuentra completamente implementado, con efectividad en la conformidad con los requisitos puede no ser necesaria la auditoría durante Etapa 2. Sin embargo, el informe de auditoría incluirá los hallazgos correspondientes en caso que las condiciones observadas previamente en Etapa 1 no se mantengan como parte de la Etapa 2.

El intervalo entre la Etapa 1 y la Etapa 2 no deberá ser mayor a 6 meses, en caso que el plazo exceda del período señalado, Etapa 1 deberá repetirse.

Certificación de seguridad de la información.

En esta etapa de la auditoría, el Organismo de Certificación debe obtener documentación sobre el diseño del SGSI cubriendo la documentación requerida en ISO / IEC 27001.

El objetivo de la auditoría de Etapa 1 es obtener una comprensión suficiente del diseño del SGSI, el contexto de la organización del cliente, la evaluación de riesgos y el tratamiento de los riesgos

del SGSI (incluidos los controles determinados), la política y objetivos de seguridad de la información y, en particular, de la preparación y planificación de la auditoría Etapa 2.
Los resultados de la etapa 1 se documentarán en un informe escrito. OSG revisará el informe de auditoría de la etapa 1 antes de decidir si procede con la etapa 2 y confirmará la competencia de los miembros del equipo de auditoría de la etapa 2; esto puede ser realizado a través del auditor que lidera el equipo que realizó la auditoría de la etapa 1 si se considera competente y apropiado o bien por la Secretaría Técnica, cuando no tenga participación en el proceso de auditoría.

5.4.2 Auditoría Etapa 2.

El propósito de la Etapa 2 es evaluar la implementación incluida la eficacia del Sistema de Gestión de la Organización. Esta Etapa se debe realizar preferentemente de manera presencial, en las instalaciones del Cliente y debe incluir al menos:

a) De la Dirección en relación con las políticas de la información y las evidencias de la conformidad con todos los requisitos de la norma de referencia u otro documento normativo aplicable.
b) Identificación de roles y responsabilidades;
c) La realización de actividades de seguimiento, medición, informe y revisión con relación a los objetivos y metas de desempeño clave coherentes con las expectativas de la norma de referencia u otro documento normativo aplicable.
d) El Sistema de Gestión del Cliente y su desempeño en relación con el cumplimiento de la legislación.
e) El control operacional de los procesos del Cliente.
f) Las Auditorías Internas y la Revisión por la Dirección.
g) La responsabilidad con su Cliente.
h) Gestión de Riesgos.
i) Comprensión de la organización y de su contexto y expectativas de las partes interesadas.
j) Evaluación del cumplimiento con los requisitos legales.
k) Eliminación de peligros y reducción de los riesgos de acuerdo al Sistema de Gestión solicitado para la certificación.

Previo a la realización de la auditoría en sitio se realizará una reunión con el Equipo Auditor para establecer los roles, así como de forma práctica realizar las actividades de reunión de apertura y cierre, comportamiento del equipo, puntualización de los documentos que el proceso requiere, tipo de cliente, características de la zona, todo tipo de información para la realización de la auditoría con el objetivo de fomentar una formación previa del Equipo Auditor.

El Equipo Auditor evalúa preferentemente in situ (Etapa II de la Auditoría de Certificación) el Sistema de Gestión del auditado para determinar su conformidad con los requisitos normativos establecidos y la confianza que brinda por los servicios suministrados a sus Clientes y Organización, teniendo en cuenta lo establecido en los procedimientos de auditoría de OSG y contractualmente.

En los casos de naturaleza extraordinaria en los cuales no sea posible realizar la visita de manera presencial, esta etapa podrá realizarse a distancia de acuerdo a los requisitos establecidos en el procedimiento de Auditorias a Distancia **PE-OSG 17**, garantizando que aun cuando se realice mediante esta técnica, los requisitos de certificación inicial serán auditados en su totalidad, incluyendo el recorrido en tiempo real de las instalaciones; lo anterior bajo la consideración que una

vez reestablecidas las condiciones para poder realizar la visita en sitio, se agendará una auditoría de seguimiento en las instalaciones del cliente en un plazo no mayor a 6 meses.

El Equipo Auditor le comunica al Cliente, en la reunión de cierre de la Auditoría de Certificación inicial, modificación del alcance o de recertificación, los resultados de la auditoría y hace entrega de los hallazgos detectados, solicitando al cliente el análisis de las causas de las no conformidades y su tratamiento con acciones correctoras y correctivas que den solución.

El cierre a las no conformidades se realizará en un plazo no mayor de 30 días naturales para las no conformidades mayores y no mayor de 90 días naturales para las menores, en un Informe Cierre de Acciones Correctivas, que deberá entregar al auditor líder a través de la Secretaría Ejecutiva de OSG en un plazo no mayor de 30 días naturales posteriores a la fecha de la reunión de cierre de la Etapa II de la auditoría, así como las evidencias de implementación de las acciones según lo planificado en los plazos establecidos.

El auditor hace de conocimiento al Cliente, que el Comité de Decisiones se reúne el primer martes de cada mes o antes de forma remota para realizar la toma de decisión sobre la Certificación, misma que se entregara máximo a los cinco (5) días naturales, de haber sido realizada la toma de decisión.

La verificación de las acciones correctoras y correctivas contenidas en el Informe Cierre de Acciones Correctivas entregado por el Cliente son revisadas por el Auditor Líder para comprobar si las mismas satisfacen el cierre de las no conformidades detectadas contando para ello con cinco (5) días naturales para dar respuesta al cliente, en caso que las acciones correctoras y correctivas no satisfacen el cierre de las no conformidades el Cliente cuenta con el termino de diez (10) naturales para presentar su nuevo Informe Cierre de Acciones Correctivas y el Auditor Líder con igual termino para dar respuesta, en caso de repetirse el ciclo la Secretaría Ejecutiva valorara con el Cliente tal situación.

La verificación de la eficacia de las acciones correctoras y correctivas emprendidas por el Cliente para dar solución a las no conformidades detectadas en un proceso de certificación inicial o de ampliación de alcance, siempre que no implique ésta última la recertificación, se realiza en la(s) siguiente(s) auditoría(s) de vigilancia.

La verificación de la eficacia de las acciones se realizará in situ por el Auditor Líder en aquellos casos que las acciones correctoras y correctivas implementadas se deriven de una violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias o cualquier no conformidad detectada en auditorías de recertificación, que deben evidenciar la solución eficaz de las causas en un plazo no mayor de treinta (30) días naturales posteriores a la fecha de la reunión de clausura de la Etapa II de la auditoría de certificación..

De no solucionarse el cierre de las no conformidades que constituyan una violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias o cualquier no conformidad detectada en auditorías de recertificación en el plazo reglamentado debe analizarse por Secretaría Ejecutiva las causas y la toma de decisión correspondiente por el incumplimiento de este requisito a causa de la extemporaneidad de los resultados auditados, pudiendo establecer si se considera un nuevo plazo no mayor de sesenta (60) días naturales posteriores a la fecha de la reunión de clausura de la Etapa II de la auditoría de certificación.

De no evidenciar el cierre de las no conformidades referenciadas se podría proponer al Comité de Decisiones la No Concesión o Mantenimiento del Certificado por la imposibilidad de evidenciar el cierre de las no conformidades detectadas en el plazo establecido o por no poder evidenciar la implantación del sistema conforme a los requisitos establecidos como criterio de auditoria, por incumplimientos graves.

Consideraciones adicionales por alcance de certificación.

Certificación Antisoborno.

En relación al Sistema de Gestión Antisoborno, la auditoría inicial de Etapa 2 y la posterior auditoría de seguimiento de la Certificación tienen como objeto confirmar la eficacia del Sistema de Gestión Antisoborno para prevenir la posibilidad de soborno y para realizar el seguimiento de los controles (e indicadores); por ejemplo, que son, y permanecen, adecuados a su propósito.

La mayoría de los procesos de soborno hasta la fecha involucran el uso de socios comerciales (intermediarios como agentes de ventas, consultores o similares). El Equipo Auditor deberá confirmar que el Cliente ha identificado y llevado a cabo un nivel adecuado de diligencia debida basada en el riesgo, para cada uno de sus socios comerciales identificados y que los está gestionando en consecuencia.

Además, la auditoría deberá revisar cómo el Cliente se asegura de que sus asociados, donde exista un riesgo de soborno mayor que bajo, hayan implementado sus propios controles contra el soborno o hayan adoptado los controles contra el soborno del Cliente (ISO 37001 sección 8.5). Uno de los principios de la evaluación de riesgos para antisoborno dice que "*la evaluación de riesgos que aplica a las operaciones nacionales de una organización comercial, podría no ser apropiada cuando inicia sus actividades en un nuevo mercado en una parte del mundo en la que no ha hecho negocios antes".*

OSG ofrece como política una certificación global para una actividad específica del Cliente, la auditoría realizada del Sistema de Gestión Antisoborno, deberá ofrecer confianza en que el proceso de evaluación de riesgos de soborno de la organización (Cliente) puede demostrar que garantiza ser lo suficientemente sólido e integrador como para tratar los cambios en las operaciones geográficas, por ejemplo al considerarse posibles nuevas oportunidades de mercado, nuevas ubicaciones de las operaciones, la cultura empresarial local, el equipo de administración, ventas, marketing, compras, cadena de suministro y fabricación.

Certificación de seguridad de la información.

Como parte de las actividades a realizar durante la etapa 2, se evaluará la implementación efectiva del SGSI, como objetivo de esta etapa se confirmará que la organización cliente se adhiere a sus propias políticas, objetivos y procedimientos.

Para hacer esto, la auditoría se centrará en los siguientes aspectos:

a) liderazgo de la alta dirección y compromiso con la política de seguridad de la información y los objetivos de seguridad de la información;

b) los requisitos de documentación enumerados en ISO / IEC 27001;
c) evaluación de los riesgos relacionados con la seguridad de la información y que las evaluaciones produzcan resultados consistentes, resultados válidos y comparables si se repiten;
d) determinación de objetivos de control y controles basados en la evaluación de riesgos de seguridad de la información y los procesos para el tratamiento de riesgos;
e) desempeño de la seguridad de la información y la efectividad del SGSI, evaluando contra los objetivos de seguridad de la información;
f) relación entre los controles determinados, la Declaración de Aplicabilidad y los resultados de la evaluación de riesgos de seguridad de la información y el proceso de tratamiento de riesgos y la política de seguridad de la información y sus objetivos;
g) implementación de controles de acuerdo a ISO 27001, teniendo en cuenta el contexto externo e interno y los riesgos relacionados, el monitoreo, medición y análisis de la seguridad de los procesos y controles aplicables a la información de la organización, para determinar si se encuentran implementados y son efectivos y el cumplimiento de sus objetivos declarados de seguridad de la información;
h) programas, procesos, procedimientos, registros, auditorías internas y revisiones de la efectividad del SGSI para asegurar que estos son trazables a las decisiones de la alta gerencia y a la política de seguridad de la información y sus objetivos.

5.4.3 Auditorías de Vigilancia.

La auditoría de vigilancia a la certificación tiene la finalidad de confirmar que se mantienen las condiciones que dieron lugar a la certificación. Las auditorías de vigilancia deben realizarse al menos una vez al año, excepto en los años de recertificación. La fecha de la primera auditoría de vigilancia 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. La fecha de la segunda auditoría de vigilancia podrá realizarse hasta el mes veintiséis (26), contados a partir del día inmediato siguiente a la fecha en que se tomó la decisión de otorgar la Certificación.

La vigencia del certificado será de tres (3) años, por lo que la Secretaría Ejecutiva deberá programar auditorías de vigilancia anual durante la vigencia de la certificación tomando como base la fecha de otorgamiento de la certificación, acordando con el Cliente la fecha para realizar la auditoría de vigilancia y también coordinará la designación del grupo auditor.

La auditoría de vigilancia debe contener al menos los siguientes elementos del sistema, pero debe considerar el evaluar, cuando menos:

a) Auditorías Internas y la Revisión por la Dirección, requisitos de la documentación, planificación, seguimiento y medición, mejora, revisión y logro de objetivos.
b) Evaluar la documentación del Sistema de Gestión de la Organización (Procedimientos de Gestión).
c) Revisión de las acciones tomadas sobre no conformidades levantadas durante la auditoría previa.
d) Quejas, cambios en la Organización.
f) Uso del logo de OSG y cualquier referencia a la certificación.

El Comité de Decisiones, dependiendo de los resultados de Auditoría presentados, podrá determinar la necesidad de que el plazo para la realización de las auditorías de vigilancias sea

modificado, incrementando la frecuencia de las mismas en función de las no conformidades, o cuando se trata de Clientes cuyo sistema este implantado en varios sitios, esto con respecto a lo establecido en el contrato correspondiente. En estos casos, la Secretaría Ejecutiva deberá notificarlo por escrito al Cliente.

El Cliente tendrá la obligación de informar por escrito a la Secretaría Ejecutiva cualquier cambio que pretenda realizar al Sistema de Gestión certificado con el fin de considerar si es necesario llevar a cabo una auditoría extraordinaria, basada en la magnitud del cambio y el impacto sobre el Sistema de Gestión certificado.

Los resultados de las vigilancias se reportan al Cliente por la Secretaría Ejecutiva de OSG en un informe emitido por el Equipo Auditor **RPE-OSG 01.11** Informe de Auditoría relacionado con el mantenimiento de los requisitos bajo los cuales se concedió el Certificado, sujeto a revisión y decisión según proceda acorde al juicio fundamentado del Equipo Auditor. Posteriormente al cierre de los hallazgos en los tiempos reglamentados por OSG se emitirá la decisión sobre la certificación.

Consideraciones adicionales por alcance de certificación

Certificación de seguridad de la información.

Los programas correspondientes a las auditorías de vigilancia de un SGSI contemplan por lo menos, lo siguiente:

a) los elementos de mantenimiento del sistema, como la evaluación y el control de riesgos de seguridad de la información, mantenimiento, auditoría interna del SGSI, revisión de la gestión y medidas correctivas;
b) comunicaciones de terceros como lo requiere la norma ISO / IEC 27001 y otros documentos requeridos para la certificación;
c) cambios en el sistema de gestión documentado;
d) áreas sujetas a cambios;
e) requisitos seleccionados de acuerdo a la norma ISO / IEC 27001;
f) otras áreas involucradas con la seguridad de la información seleccionadas según corresponda.
g) En caso de existir problemas de seguridad relacionados con el análisis de riesgos e impacto se debe considerar una revisión del análisis y tratamiento de los mismos.

Durante la auditoría de vigilancia, se debe indicar en el informe la evaluación, como mínimo de los siguientes aspectos:

a) la efectividad del SGSI con respecto al logro de los objetivos de la información del cliente, así como la política de seguridad;
b) el funcionamiento de los procedimientos para la evaluación periódica y la revisión del cumplimiento de la legislación y normativa(s) aplicables a la seguridad de la información;
c) cambios en los controles determinados y cambios resultantes en la Declaratoria de Aplicabilidad;
d) implementación y efectividad de los controles de acuerdo con el programa de auditoría.
e) Verificar los registros de quejas y/o apelaciones
f) Seguimiento a los hallazgos registrados durante auditorías previas (internas o externas)

Las auditorías de vigilancia pueden combinarse con auditorías de otros sistemas de gestión; cuando suceda lo anterior se indicará debidamente en el informe los aspectos relevantes para cada Sistema de Gestión.

5.4.4 Recertificación.

La Organización certificada debe presentar la Solicitud de Servicio cinco (5) meses antes del vencimiento del certificado junto con los documentos enumerados en dicha solicitud para su proceso por la Secretaría Ejecutiva.

Las actividades de recertificación pueden incluir el llevar a cabo una auditoría de Etapa 1, en aquellos casos en que haya habido cambios significativos en el Sistema de Gestión del Cliente, en su Organización o en el contexto en el que se desarrolla su SG (P.ej. cambios en la legislación aplicable).

Para considerar renovada la certificación, requiere la realización de la auditoría, el cierre de cualquier no conformidad mayor detectada durante la misma y la decisión positiva sobre la recertificación antes de expirar el plazo de vigencia señalado en el certificado anterior.

En caso de no cumplirse con los requisitos, el Certificado pierde su validez en la fecha señalada y se publica la cancelación del mismo en el sitio web de OSG.

En casos excepcionales (demora en la obtención de los avales que no dependen del Cliente, cambios estructurales o funcionales en la entidad u otras causas que OSG pueda considerar), se podrá restaurar la certificación vencida dentro de los 6 meses siguientes, siempre y cuando se hayan completado satisfactoriamente las actividades de recertificación pendiente de otro modo, se debe realizar mínimo una Etapa 2.

La fecha de vigencia del certificado debe ser la fecha de la decisión de la nueva certificación o una posterior, y la fecha de expiración se debe basar en el ciclo de certificación anterior.

Consideraciones adicionales por alcance de certificación.

Certificación de seguridad de la información.

La recertificación correspondiente a la certificación en materia de Seguridad de la Información, se realizará de acuerdo a lo previsto, sin embargo, se debe considerar que el tiempo permitido para implementar acciones correctivas debe ser consistente con la severidad de la no conformidad y el riesgo de seguridad de la información asociado.

5.4.5. Auditorías Especiales.

5.4.5.1. Ampliación de alcance.

En caso de recibir la solicitud por parte del cliente para ampliar el alcance de una certificación ya otorgada, la secretaría técnica realizará la revisión de dicha solicitud con la finalidad de determinar la necesidad de realizar una auditoría adicional o bien, contemplar esta ampliación durante las auditorías de vigilancia programadas al cliente o bien durante un seguimiento.

5.4.5.2. Auditorías con notificación a corto plazo.

En caso de requerirse la investigación a profundidad de alguna queja recibida sobre una certificación otorgada; si existieran cambios en las certificaciones que se consideren de importancia su validación; o en el caso de dar seguimiento de vigilancia a aquellos clientes que se encuentren con una certificación suspendida, la secretaría técnica puede considerar la realización de alguna visita notificada a corto plazo o incluso sin notificar, con la intención de revisar las condiciones antes descritas

Consideraciones adicionales por alcance de certificación.

Certificación de seguridad de la información.

Las auditorías especiales de SGSI estarán sujetas a una disposición especial si un Cliente realiza modificaciones importantes en su sistema o si se producen otros cambios que podrían afectar la base de su certificación.

5.5. Realización de la auditoría:

En esta Etapa se describen los pasos para llevar a cabo el proceso de auditoría.

5.5.1. Reunión de apertura.

El auditor líder inicia con una reunión, donde circula el registro **RPE-OSG** 01.8 Lista de Asistencia, esta reunión tiene la finalidad de:

a) Presentar a los participantes, incluida una breve descripción de sus roles.
b) Confirmación del alcance de la certificación.
c) Confirmación del plan de auditoría (incluyendo el tipo y el alcance de la auditoría, los objetivos y los criterios), cualquier cambio, y otros acuerdos pertinentes con el Cliente, tales como la fecha y la hora de la reunión de cierre, las reuniones intermedias entre el Equipo Auditor y la dirección del Cliente.
d) Confirmación de los canales de comunicación formales entre el Equipo Auditor y el Cliente.
e) Confirmación de que están disponibles los recursos y las instalaciones que requiere el Equipo Auditor.
f) Confirmación de los temas relativos a la confidencialidad y Compromiso de los Miembros del Equipo Auditor reflejado en el RPE-OSG 09.3.
g) Confirmación de los procedimientos de protección, emergencia y seguridad ocupacional, para el Equipo Auditor.
h) Confirmación de la disponibilidad, de los roles y de la identidad de los guías y observadores.
i) El método para presentar la información, incluida cualquier categorización de los hallazgos de la auditoría.
j) Información sobre las condiciones bajo las cuales la auditoría puede darse por terminada prematuramente.
k) Confirmación de que el Líder y los miembros del Equipo Auditor que representan al Organismo de Certificación son responsables de la auditoría y que deben controlar la ejecución del plan de auditoría, incluidas las actividades y las líneas de investigación de la auditoría.
l) Confirmación del estado de los hallazgos de la revisión o auditoría anterior, cuando corresponda.

m) Los métodos y procedimientos que se van a utilizar para llevar a cabo la auditoría sobre la base de un muestreo.
n) Confirmación del idioma que se utilizará durante la auditoría.
o) Confirmación de que durante la auditoría se mantendrá informado al Cliente sobre el progreso de la auditoría y sobre cualquier problema.
p) Oportunidad para que el Cliente haga preguntas.
q) Entrega al auditado de **RPE-OSG 01.13** Encuesta de Satisfacción del Cliente y el **RPE-OSG 03.3** Evaluación del Desempeño del Equipo Auditor por el Cliente.

El Auditor Líder debe utilizar y llenar el registro **RPE-OSG 01.9** Reunión de Apertura y Cierre, que detalla los puntos anteriores. A partir de la reunión de apertura y en cualquier fase de la auditoría, si a juicio del Auditor Líder es necesario considerar la suspensión de la auditoría cuando exista una posible afectación a la integridad o la seguridad del Equipo Auditor, se debe notificar a OSG quien inmediatamente informará las razones para tomar esta decisión a la Organización auditada.

5.5.2 Recorrido por las instalaciones.

Posterior a la reunión de apertura el Equipo Auditor hará un recorrido por las instalaciones de la Organización a auditar, guiados por la(s) persona(s) asignada(s), esto tiene como finalidad ver el aspecto general de las mismas y para que el Equipo Auditor ubique sus diferentes áreas; así como tener un panorama general de la actitud de la Organización hacia el Sistema de Gestión. Este recorrido puede ser no aplicable siempre y cuando el Equipo Auditor lo considere.

En los casos que aplique la realización de una auditoría a distancia, el recorrido por las instalaciones deberá realizarse por los medios que indique la organización, garantizando en todo momento contar con acceso virtual por parte del equipo auditor y con disponibilidad del personal a cargo para realizar las entrevistas según se requiera.

5.5.3 Ejecución de la auditoría.

El Auditor Líder debe preparar la documentación necesaria y suficiente para la revisión de la auditoría, la cual incluye lo siguiente:

1. RPE-OSG 01.4 Plan de Auditoría.
2. RPE-OSG 01.6 Informe Cierre de Acciones Correctivas.
3. RPE-OSG 01.8 Lista de Asistencia.
4. RPE-OSG 01.9 Reunión de Apertura y Cierre
5. Listas de chequeo, de acuerdo al alcance de la certificación:
   RPE-OSG 01.10 Lista de Chequeo ISO 28000.
   RPE-OSG 01.14 Lista de Chequeo ISO 37001.
   RPE-OSG 01.15 Lista de Chequeo ISO 27001.
   RPE-OSG 01.16 Lista de Chequeo ISO 22301.
   RPE-OSG 01.17 Lista de Chequeo ISO 22000.
6. RPE-OSG 01.11 Informe de Auditoría.
7. RPE-OSG 01.12 Hallazgos de Auditoría.
8. RPE-OSG 01.13 Encuesta de Satisfacción del Cliente.
9. RPE-OSG 03.3 Evaluación del desempeño del Equipo Auditor por el Cliente.

El Equipo Auditor siempre debe apegarse a las indicaciones del Plan de Auditoría y al objetivo de la misma, además deberán verificar los aspectos legales, reglamentarios y técnicos relacionados con el producto o servicio.

El propósito de la auditoría es recopilar evidencia objetiva con respecto a la eficacia del Sistema de Gestión de la Organización a través de entrevistas, observación de operaciones, actividades de evaluación, evidencias, revisión de documentos, de registros de acuerdo al alcance de la auditoría; asimismo tomando notas y referencias en las Lista de Chequeo.

Para lograr esto, es importante realizar las siguientes actividades:

1. Registrar la evidencia de conformidad en las Lista de Chequeo.
2. Verificación de la documentación de la implantación del Sistema de Gestión o parte del mismo (manual, procedimientos e instrucciones de trabajo) para determinar si está completa y es adecuada.
3. Comprobación de que se siguen los procedimientos e instrucciones de trabajo.
4. Confirmación de la competencia de inspectores y operadores de procesos especiales (calificación y certificación).
5. Confirmación del cumplimiento de requisitos legales y reglamentarios.
6. Examen aleatorio de muestras de trabajo (registros, productos, cálculos, dibujos, etc.)
7. Verificación de controles y registros de procesos.
8. Recolección de evidencias objetivas.
9. Para auditorías de vigilancia, verificar el uso apropiado del logo y Certificado de OSG.
10. Con respecto a las no aplicabilidades declaradas por la Organización auditada, el auditor verificará que dichas exclusiones en realidad apliquen.
11. Para los dos casos anteriores, el auditor hará constar dichas verificaciones en el Informe de Auditoría.

La ejecución de la auditoría es un ejercicio de muestreo, por lo tanto, es muy importante que el auditor esté seguro de que las muestras que se tomen sean representativas del total que se está examinando. En caso de que el auditor determine un hallazgo y su clasificación y tenga alguna duda al respecto, deberá consultarlo con el Auditor Líder. Cabe hacer mención que los hallazgos de las auditorías de Etapa 1, se identifican en conformidad y no conformidad.

Los hallazgos para las demás auditorías (Etapa 2, recertificación, vigilancia, ampliación, reducción, restauración, notificación a corto plazo, seguimiento/extraordinaria) se clasifican en conformidades, No Conformidades Mayores, No Conformidades Menores y Observaciones (Oportunidades de Mejora).

Consideraciones adicionales por alcance de certificación

Certificación de seguridad de la información.

Durante la auditoría de certificación el equipo auditor, deberá:

a) exigir al cliente que demuestre que la evaluación de los riesgos relacionados con la seguridad de la información es relevante y adecuada para la operación del SGSI dentro del alcance del SGSI;

b) establecer si los procedimientos del cliente para la identificación, examinación y evaluación de los riesgos relacionados con la seguridad de la información y los resultados de su implementación son consistentes con la política, objetivos y metas del cliente.

5.5.4. Reunión del Grupo Auditor.

El Auditor Líder convoca al Equipo Auditor a reuniones intermedias durante el proceso de la auditoría. Dichas reuniones tienen como objetivo:

a) Intercambiar información sobre los hallazgos encontrados basados en evidencias objetivas.
b) Definir, evaluar y documentar los hallazgos de auditoría. Siempre con el sustento de evidencia suficiente para la determinación de los mismos.
c) Coordinar actividades para asegurar el cumplimiento de los objetivos diarios.
d) Aclarar dudas que se presenten durante la auditoría.
e) Cuando por causas inesperadas se tenga que cambiar la agenda de auditoría, el auditor líder convoca a una reunión especial para explicar el cambio y la razón del mismo.
f) Al término de la auditoría se reúne el Equipo Auditor para recabar toda la información y elaborar el **Informe de Auditoría** y **Hallazgos de Auditoría**.

El **RPE-OSG 01.11** Informe de Auditoría debe incluir, cuando sea necesario, si se requiere de una auditoría completa adicional, una auditoría de seguimiento o la presentación de un plan de acciones sobre hallazgos detectados que serían revisadas en la siguiente Auditoría de Vigilancia.

El Equipo Auditor debe analizar toda la información y las evidencias de auditoría obtenidas durante las Etapas 1 y 2, para revisar los hallazgos de auditorías y acordar las conclusiones de la auditoría.

5.5.5 Reunión de Cierre.

Una vez concluida la auditoría y elaborado el Informe de Auditoría y los Hallazgos de Auditoría (cuando aplica), el Auditor Líder convoca a la reunión de cierre al Equipo Auditor y al personal auditado, el Auditor Líder es responsable de llevar a cabo la reunión de cierre a nombre del Equipo Auditor, agradeciendo las atenciones y facilidades recibidas durante el proceso de auditoría y circulando **RPE-OSG 01.8** Lista de Asistencia.

El objetivo de la reunión es informar a los auditados, el resultado de la auditoría e informar los hallazgos; si el responsable de la auditoría por parte de la Organización auditada está de acuerdo con los hallazgos declarados, debe firmar el Informe de Auditoría en su caso realizar una aceptación vía correo electrónico, asimismo el Auditor Líder hace entrega al auditado de una copia de la documentación correspondiente.

En caso de documentar hallazgos, se debe instruir a la Organización auditada que debe analizar las causas y describir las correcciones y las acciones correctivas realizadas para eliminar dichas no conformidades, de acuerdo a la propia metodología de la Organización auditada y respetando los tiempos establecidos en el apartado 5.6. los cuales deberán de ser descritos en el **RPE-OSG 01.12** Hallazgos de Auditoría, los cuales deberán ser entregados de manera física o electrónica.

Por el contrario, si el responsable de atender la auditoría no está de acuerdo con algún hallazgo, el Auditor Líder escuchará su fundamento y en caso de presentar evidencia de cumplimiento procederá

a cancelar el hallazgo, en caso de no llegar a un acuerdo le indicará al responsable auditado que escriba sus argumentos fundamentándolos en el mismo informe, así mismo informarle sobre el Procedimiento de Quejas y Apelaciones.

El auditor líder debe concluir con la Reunión de Cierre e informar inmediatamente a la Secretaría Ejecutiva acerca de la situación, antes de dar por terminada la reunión de conclusiones se hace entrega por el auditado del **RPE-OSG 01.13** Encuesta de Satisfacción del Cliente y el **RPE-OSG 03.3** Evaluación del Desempeño del Equipo Auditor por el Cliente.

Es importante que el Equipo Auditor nunca entre en discusión con el auditado, el Auditor Líder debe recordarle al auditado que debe presentar a la Secretaría Ejecutiva de OSG en un plazo no mayor de 30 días naturales posteriores a la fecha de la reunión de cierre de la **Etapa II** el **REPE-OSG 01.5** Informe Cierre de Acciones Correctivas el que contempla el análisis de las causas de las no conformidades y su tratamiento con acciones correctivas que den solución y cierre a las no conformidades mayores y para el caso de las no conformidades menores el auditado que debe presentar a la Secretaría Ejecutiva de OSG en un plazo no mayor de 90 días naturales posteriores a la fecha de la reunión de cierre de la **Etapa II** de la auditoría. La implementación de las acciones a las no conformidades menores será revisada en la siguiente visita.

La verificación de las correcciones y acciones correctivas contenidas en el Informe Cierre de Acciones Correctivas entregado por el Cliente son revisadas por el Auditor Líder para comprobar si las mismas satisfacen el cierre de las no conformidades detectadas contando para ello con cinco (5) días hábiles para dar respuesta al Cliente, en caso que las acciones correctivas no satisfacen el cierre de las no conformidades el Cliente cuenta con el termino de diez (10) naturales para presentar su nuevo Informe Cierre de Acciones Correctivas y el Auditor Líder con igual término para dar respuesta, en caso de repetirse el ciclo la Secretaría Ejecutiva valorará con el Cliente tal situación.

La verificación de la eficacia de las correcciones y acciones correctivas emprendidas por el Cliente para dar solución a las no conformidades detectadas en un proceso de certificación inicial o de ampliación de alcance, siempre que no implique ésta última la recertificación, se realiza en la(s) siguiente(s) auditoría(s) de vigilancia.

Se exceptúa de lo dispuesto en la verificación de la eficacia de las acciones correctivas implementadas para dar solución a no conformidades que constituyan violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias o cualquier no conformidad detectada en auditorías de recertificación, que deben evidenciar la solución eficaz de las causas en un plazo no mayor de treinta (30) días naturales posteriores a la fecha de la reunión de clausura de la **Etapa II** de la auditoría de certificación. La verificación de la eficacia de las acciones se realizará in situ por el auditor líder.

De no solucionarse el cierre de las no conformidades que constituyan violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias o cualquier no conformidad detectada en auditorías de recertificación en el plazo reglamentado debe analizarse por Secretaría Ejecutiva las causas y la toma de decisión correspondiente por el incumplimiento de este requisito a causa de la extemporaneidad de los resultados auditados.

Pudiendo establecer si se considera un nuevo plazo no mayor de sesenta (60) días naturales posteriores a la fecha de la reunión de clausura de la **Etapa II** de la auditoría de certificación, de no evidenciar el cierre de las no conformidades referenciadas.

El Auditor Líder hace de conocimiento al Cliente, que el Comité de Decisiones se reúne el primer martes de cada mes o antes de forma remota para realizar la dictaminación de la certificación, misma que se entregara máximo a los cinco (5) días naturales, de haber sido realizada la dictaminación.

Consideraciones adicionales por alcance de certificación

Certificación de seguridad de la información.

Además de los requisitos regulares, el informe de auditoría para las auditorías de SGSI deberá indicar el alcance del SGSI, las desviaciones del plan de auditoría, así como el análisis de riesgos correspondiente a la seguridad de la información de la organización cliente.

De tal manera que dicho informe deberá ser lo suficientemente detallado para facilitar y respaldar la decisión de certificación, conteniendo la siguiente información:

a) seguimientos importantes de auditoría seguidos y metodologías de auditoría utilizadas;
b) observaciones realizadas durante la auditoría;
c) comentarios sobre la conformidad del SGSI de la organización cliente respecto a los requisitos de certificación indicando las no conformidades registradas en caso de encontrarse; además de contar con una referencia a la versión de la Declaración de Aplicabilidad aplicable;
d) Recomendación del equipo auditor respecto a si el SGSI de la organización cliente debe certificarse o no, dicha decisión deberá estar fundamentada con la información recopilada durante la auditoría y registrada en el informe de auditoría correspondiente.

El informe debe incluir las listas de verificación, observaciones, registros o las notas del equipo auditor; se deberá señalar la utilización de métodos o técnicas empleadas durante la auditoría, así como la información correspondiente al muestreo evaluado, en caso de requerirse.

El informe considerará la adecuación de la organización interna y los procedimientos adoptados por el cliente para dar confianza en el SGSI.

5.5.6 Paquete de auditoría.

El Auditor Líder debe reunir la documentación de la auditoría y entregarla a la Secretaría Técnica a más tardar cinco (5) días naturales después de concluida la auditoría, el paquete de auditoría deberá contener:

1. RPE-OSG 01.4 Plan de Auditoría.
2. RPE-OSG 01.6 Informe Cierre de Acciones Correctivas.
3. RPE-OSG 01.8 Lista de Asistencia.
4. RPE-OSG 01.9 Reunión de Apertura y Cierre
5. Listas de chequeo, de acuerdo al alcance de la certificación:
   RPE-OSG 01.10 Lista de Chequeo ISO 28000.
   RPE-OSG 01.14 Lista de Chequeo ISO 37001.

RPE-OSG 01.15 Lista de Chequeo ISO 27001.
RPE-OSG 01.16 Lista de Chequeo ISO 22301.
RPE-OSG 01.17 Lista de Chequeo ISO 22000.

6. RPE-OSG 01.11 Informe de Auditoría.
7. RPE-OSG 01.12 Hallazgos de Auditoría.
8. RPE-OSG 01.13 Encuesta de Satisfacción del Cliente.
9. RPE-OSG 03.3 Evaluación del desempeño del Equipo Auditor por el Cliente.

Una vez completo el paquete de auditoría Secretaría Técnica verificará su contenido a través del registro **RPE-OSG 01.7** Revisión Técnica. En caso de que la información este incompleta, se solicita la información faltante al Auditor Líder.

Si como resultado de la revisión se obtiene un resultado de 4 puntos como mínimo, la Secretaría Ejecutiva propone el otorgamiento del certificado del Sistema de Gestión en composición reducida, si se obtiene un resultado de 3.9 puntos o inferior, la Secretaría Ejecutiva propone se gestione la decisión sobre el otorgamiento del certificado del Sistema de Gestión en sesión presencial.

El Equipo Auditor debe emitir a la Secretaría Ejecutiva en el **RPE-OSG 01.11** Informe de Auditoría la propuesta para la decisión sobre la certificación, con una de las alternativas siguientes:

a) Otorgar el certificado por considerar cerradas todas las no conformidades, solo es válida esta alternativa para auditorías de recertificación.
b) Conceder o mantener el certificado basado en el cumplimiento y adecuación de las acciones correctivas, con notas para la siguiente auditoría de vigilancia, para verificar la eficacia de las acciones correctivas tomadas en las no conformidades y la objetividad de la planificación de las acciones emprendidas, siempre que las no conformidades no constituyan violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias las que obligatoriamente deben quedar debidamente cerradas antes de proponer al Comité de Decisiones la concesión del certificado.
c) Conceder o mantener el certificado con una auditoría de vigilancia extraordinaria a efectuar dentro de los seis (6) meses posteriores a la fecha de implementación de acciones correctivas que requieran de acumular un mayor número de evidencias, o seguimiento de inversiones que excedan el plazo de noventa (90) días naturales estipulado para el cierre de no conformidades, siempre que las no conformidades no constituyan violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias, las que obligatoriamente deben de quedar debidamente cerradas antes de proponer al Comité de Decisiones la concesión o mantenimiento del certificado. Esta auditoría de vigilancia extraordinaria condicionaría el mantenimiento del certificado o su cancelación, quedando el Cliente obligado a efectuar una nueva solicitud en caso de que se decida cancelar el certificado. En casos excepcionales y por motivos bien argumentados, el Comité de Decisiones podría autorizar una prórroga de dicho plazo, previa fundamentación documentada.
d) No conceder o mantener el certificado por la imposibilidad de evidenciar el cierre de las no conformidades detectadas en el plazo establecido o por no poder evidenciar la implantación del sistema conforme a los requisitos establecidos como criterio de auditoría, por incumplimientos graves.

Una vez que la información está completa, la Secretaría Ejecutiva coloca en formato PDF la documentación en la carpeta de Comité de Decisiones, para que se proceda de acuerdo con lo

establecido en el punto 5.7 del presente procedimiento. El informe de la auditoría deberá ser enviado al Cliente por medio de la Secretaría Ejecutiva junto con las listas de asistencia y los formatos de hallazgos en un plazo no mayor a 10 días hábiles después de concluida la auditoría. Se exceptúa de la entrega al Cliente lo contenido en el Anexo A del Informe de Auditoría.

Cada vez que se concluya una Fase del Proceso de Certificación de la que se exceptúa la decisión sobre la certificación, OSG por medio del personal que le corresponda entregará al Cliente la encuesta de satisfacción sobre el servicio proporcionado. La encuesta llenada por parte del Cliente será entregada a la Secretaría Técnica. La información derivada de la aplicación de la encuesta será revisada y analizada por la Secretaría Técnica y presentada a la Dirección como parte de la revisión anual para revisión de cumplimiento con las políticas y objetivos de OSG.

Cada vez que concluya la **Fase II** auditoría en sitio, esté completa, entregada a Secretaría Técnica y revisada por esta toda la información, se convocará por la misma a un taller con la participación del equipo auditor, padrón de OSG y personal de la Secretaría para evaluar el desempeño de la realización de la auditoría efectuada con el objetivo de retroalimentar el sistema de gestión en busca de la mejora continua.

5.6. Seguimiento de los hallazgos detectados:

Como resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría, se puede declarar Conformidad, No Conformidad Mayor, No Conformidad Menor y Observaciones (Oportunidad de Mejora) o No conformidad (En el caso de Etapa 1).

No Conformidad Mayor: Se deberá entregar al Auditor Líder a través de la Secretaría Ejecutiva de OSG en un plazo no mayor de 30 días naturales posteriores a la fecha de la reunión de cierre de la Etapa 2 de la auditoría en un Informe Cierre Acciones Correctivas por el Cliente, así como las evidencias de implementación de las acciones según lo planificado en los plazos establecidos. La revisión del Informe y su implementación podrá ser realizado de manera documental, de manera remota o en sitio según sea necesario.

En caso de que las acciones tomadas no sean suficientes para solventar la No Conformidad Mayor detectada en una auditoría de certificación el paquete del Cliente no podrá entrar al Comité de Decisiones, al término del plazo si el Cliente aún no ha entregado la información el proceso de certificación iniciara de nuevo. En caso de una auditoría de vigilancia será suspendido, si en un plazo mayor a seis (6) meses las acciones no han sido suficientes para solventar la No Conformidad Mayor se cancelará el certificado.

No Conformidad Menor: Se debe enviar el Informe Cierre Acciones Correctivas elaborado por el Cliente para su revisión al Auditor Líder por Secretaría Ejecutiva, este además es revisado por la Secretaría Técnica y se envía el Informe de Auditoría a la Secretaría Ejecutiva para la toma de decisiones, en la siguiente auditoría se hará revisión a las acciones tomadas, las cuales si no son eficaces, adecuadas o atendidas podrán transformarse en una no conformidad mayor. El tiempo para enviar el Informe Cierre Acciones Correctivas no será mayor de noventa (90) días naturales después del cierre de la auditoría.

Oportunidad de Mejora (Observaciones): Se enviará un análisis por parte del Cliente a OSG para indicar su seguimiento, sin embargo, no es obligatorio implementarlas por parte del Cliente. En caso de no presentar ninguna acción se registrará como una no conformidad menor en la siguiente visita.

De no solucionarse el cierre de las no conformidades que constituyan violación de requisitos legales, reglamentarios y/o establecidos en normas mexicanas obligatorias o cualquier no conformidad detectada en auditorías de recertificación en el plazo reglamentado debe analizarse por Secretaría Ejecutiva las causas y la toma de decisión correspondiente por el incumplimiento de este requisito a causa de la extemporaneidad de los resultados auditados.

Pudiendo establecer si se considera un nuevo plazo no mayor de sesenta (60) días naturales posteriores a la fecha de la reunión de clausura de la Etapa II de la auditoría de certificación para el caso de certificaciones iniciales y para el caso de vigilancia o recertificación se iniciará un proceso de suspensión hasta en tanto las no conformidades no sean atendidas

La verificación de las acciones correctivas contenidas en el Informe Cierre Acciones Correctivas entregado por el Cliente son revisadas por el Auditor Líder para comprobar si las mismas satisfacen el cierre de las no conformidades detectadas contando para ello con cinco (5) días naturales para dar respuesta al Cliente, en caso que las acciones correctivas no satisfacen el cierre de las no conformidades el Cliente cuenta con el termino de diez (10) naturales para presentar su nuevo Informe Cierre Acciones Correctivas y el Auditor Líder con igual término para dar respuesta, en caso de repetirse el ciclo la Secretaría Ejecutiva valorara con el Cliente tal situación.

5.7 Decisión sobre la Certificación.

a) La revisión técnica del proceso de certificación de la conformidad se realiza por la Secretaría Técnica de OSG y por personal no involucrado al proceso de auditoría realizado al Cliente, calificando la conformidad con los documentos del Sistema de Gestión de OSG establecido y el desempeño del Equipo Auditor, enviando a la Secretaría Ejecutiva la documentación correspondiente y proponiendo una de las siguientes alternativas:

   - ✓ Someter a consideración del Comité de Decisiones la decisión de concesión tácita de los atributos de certificación de la conformidad.
   - ✓ Someter a análisis la decisión sobre la certificación de la conformidad en sesión presencial del Comité de Decisiones en pleno, cuando se entienda conveniente como resultado del proceso de revisión técnica, o cuando la propuesta del Equipo Auditor sea la de no otorgar o no mantener el certificado, pudiendo contar con la presencia en la sesión del Comité de Decisiones en calidad de invitados, de personal competente en el campo de actividad de los procesos a debate, con derecho a emitir criterios imparciales, pero no derecho al voto, de acuerdo al procedimiento de funcionamiento del Comité de Decisiones.

b) Toda decisión del Comité de Decisiones derivada de las propuestas anteriores se le comunica al Cliente debidamente fundamentado, procediendo a la entrega de los atributos correspondientes en caso positivo, informando públicamente de ello en el listado de entidades certificadas o en el de certificados cancelados del sitio web de OSG.

c) El Certificado tendrá una vigencia de tres (3) años, a partir de la fecha de la decisión sobre la certificación, siempre que se mantengan las condiciones bajo las cuales fue concedido, comunicado oficialmente a partir de la fecha de emisión del otorgamiento del certificado y atributos correspondientes de la certificación por la OSG.

d) Para la toma de la decisión sobre la etapa de certificación se debe de considerar el tratamiento a las No conformidades de acuerdo a lo establecido en el requisito 5.6 de este procedimiento

e) El Comité de Decisiones puede valorar la suspensión temporal por un período no mayor de seis (6) meses en el cual no se cancela la certificación del titular, pero sí el uso y divulgación de los atributos de la certificación, a partir de:

- ✓ Una medida tomada a propuesta del Equipo Auditor argumentada en el Informe de auditoría.
- ✓ El titular no permita realizar las auditorías de vigilancia o de recertificación con la periodicidad requerida.
- ✓ A solicitud del Cliente de certificación como prórroga para una auditoría planificada, por razones debidamente fundamentadas documentalmente ante la imposibilidad excepcional de cumplir algún requisito de los establecidos en el presente documento.

En caso que no se resuelvan los hallazgos que dieron lugar a la suspensión en el plazo establecido por OSG, se retira o se reduce el alcance de la certificación.

Consideraciones adicionales por alcance de certificación

Certificación de seguridad de la información.

Para la certificación correspondiente a seguridad de la información se debe considerar que además de los requisitos señalados previamente, la decisión de certificación considerará la recomendación de certificación del equipo de auditoría según lo dispuesto en su informe de auditoría de certificación.

Las personas o comités que toman la decisión de otorgar la certificación normalmente no deberían revocar una recomendación negativa del equipo auditor. Si tal situación surge, la decisión contraria a la recomendación deberá estar documentada y debidamente justificada.

La certificación no se otorgará a la organización cliente hasta que haya evidencia suficiente para demostrar que han sido atendidos los hallazgos resultantes de las revisiones gerenciales, auditorías internas y que el SGSI se encuentra implementado, mantenido y es efectivo.

5.8 Cambios en los Requisitos de Certificación.

OSG, pondrá públicamente accesible a los Clientes mediante su sitio web y otras formas de comunicación, cualquier cambio que se realice en los requisitos de certificación, detallando sus características y la fecha de su entrada en vigor, facilitando la Secretaría Ejecutiva un plazo de tiempo razonable para que los Clientes ajusten los procedimientos correspondientes en cada caso específico.

OSG, tomando en cuenta la naturaleza e importancia de los cambios o modificaciones informadas, decide sobre los cambios en la planificación y alcance de las vigilancias posteriores. Cuando ocurran cambios significativos entre la **Etapa I y II** se valorará por el Comité de Decisiones la necesidad de repetir la **Etapa I** o parte de ella. En caso que sea detectado por OSG que no se notificaron por el titular los cambios o modificaciones establecidos, podrá procederse a la aplicación de medidas.

5.9 Notificación Efectuada al Titular del Certificado.

El titular se comprometerá a investigar y resolver de manera convincente todas las notificaciones, reclamaciones y quejas provenientes de sus Clientes, o efectuadas por autoridades competentes, que puedan poner en duda la conformidad del Sistema de Gestión del titular del certificado con los requisitos de las normas aplicables al alcance del sistema. OSG puede realizar auditorías al titular bajo la forma de visitas notificadas a corto plazo o sin anunciar con el fin de investigar las quejas en respuesta a cambios, o como vigilancia de Clientes con la certificación suspendida. El titular debe disponer, y mantener accesible a OSG, el registro de dichas notificaciones, reclamaciones y quejas, así como el tratamiento dado a las mismas.

5.10 Uso del Certificados y Atributos de la Certificación del Sistema de Gestión.

Los símbolos de la Certificación (certificado y el logotipo correspondiente al Sistema de Gestión certificado) es propiedad de OSG protegido legalmente y autorizado por éste para ser otorgado y regulado por OSG, el cual establece el Procedimiento **PE-OSG 08** Contenido, Uso y Reproducción de los Documentos y Símbolos de Certificación de OSG, el mismo será entregado al Cliente en formato digital en el proceso de contratación.

Consideraciones adicionales por alcance de certificación

Certificación de seguridad de la información.
Los documentos de certificación pueden hacer referencia a normas nacionales e internacionales como fuente(s) de control establecido para controles que se determinan como necesarios en la Declaración de aplicabilidad de la organización. La referencia en los documentos de certificación debe indicarse claramente como una fuente de conjunto de control para los controles aplicados en la Declaración de aplicabilidad y no como una certificación de la misma.

5.11 Quejas.

Las quejas relacionadas con el desarrollo de los procesos de certificación en cualquiera de sus etapas, formuladas por los titulares de certificados, de Clientes de las entidades certificadas o de otras partes interesadas (en lo adelante “promovente”) serán presentadas preferentemente de forma documentada (incluyendo la vía del correo electrónico) a OSG, el cual establece el Procedimiento **PE-OSG 11** Tratamiento de las Quejas, el mismo será entregado al Cliente el formato digital en el proceso de contratación.

5.12 Apelaciones.

Las apelaciones a decisiones tomadas por el Comité de Decisiones se dirigirán al Presidente de OSG a través de la Secretaría Ejecutiva fundamentando los descargos de forma documentada, que serán resueltos en un término **No Mayor** de treinta (30) días naturales a partir de su recepción, previo análisis por el Comité de Apelaciones con el objetivo de preservar la imparcialidad de OSG, el cual establece el Procedimiento **PE-OSG 10** Tratamiento de las Apelaciones, el mismo será entregado al Cliente en formato digital en el proceso de contratación.

5.13 Confidencialidad.

OSG y los Clientes están obligados al tratamiento confidencial de la información intercambiada durante el proceso de certificación de la conformidad, salvo en los casos que se determine lo contrario por acuerdo entre los mismos, OSG establece el Procedimiento **PE-OSG 09** Confidencialidad de la Información, el mismo será entregado al Cliente en formato digital en el proceso de contratación.

5.14 Imparcialidad.

a) OSG hace evidente su compromiso con el cumplimiento de los requisitos de imparcialidad e integridad en el ejercicio de sus actividades de evaluación de la conformidad de manera imparcial, a través de un proceso de identificación, análisis, evaluación, tratamiento y contrarrestar de forma regular los riesgos relacionados con conflictos de intereses que surjan de los servicios de certificación.
b) OSG es responsable de la imparcialidad de sus actividades de evaluación de la conformidad y no permite presiones comerciales, financieras u otras que comprometan la imparcialidad, las que se encuentran establecidas en su Política de Imparcialidad.
c) OSG Asegura la imparcialidad fundamentalmente mediante:

- ✓ La firma del compromiso del Código de Ética del personal que participa en actividades de Evaluación de la Conformidad ejecutadas por OSG y por todo el personal involucrado.
- ✓ El funcionamiento eficaz de sus Comités de Decisiones, Imparcialidad y Apelaciones en base al procedimiento y requisitos establecidos en el **R-OSG** Reglamento de Certificación, así como las normativas vigentes y reglamentos de los órganos antes citados, promoviendo su difusión y cumplimiento.
- ✓ No realizar servicios de certificación a entidades relacionadas con OSG, o entidades cuyos propietarios tengan participación en el OSG.
- ✓ No ofrecer ni proporcionar consultoría en materia de sistemas de gestión.

6. Anexos.

RPE-OSG 01.1 Solicitud de Certificación.
RPE-OSG 01.2 Registro Solicitud de Certificación.
RPE-OSG 01.3 Programa de Auditoría.
RPE-OSG 01.4 Plan de Auditoría.
RPE-OSG 01.5 Informe Auditoría Documental.
RPE-OSG 01.6 Informe Cierre Acciones Correctivas.
RPE-OSG 01.7 Revisión Técnica.
RPE-OSG 01.8 Lista de Asistencia.
RPE-OSG 01.9 Reunión de Apertura y Cierre.
RPE-OSG 01.10 Lista de Chequeo ISO 28000.
RPE-OSG 01.11 Informe de Auditoría.
RPE-OSG 01.12 Hallazgos de Auditoría.
RPE-OSG 01.13 Encuesta de Satisfacción del Cliente.
RPE-OSG 01.14 Lista de Chequeo ISO 37001.
RPE-OSG 01.15 Lista de Chequeo ISO 27001.
RPE-OSG 01.16 Lista de Chequeo ISO 22301.
RPE-OSG 01.17 Lista de Chequeo ISO 22000.
Anexo A RPE-OSG 01.11 Recomendaciones del Equipo Auditor