

ÍNDICE

1. GENERAL	1
2. OBJETO Y CAMPO DE APLICACIÓN	2
3. CRITERIOS ESPECÍFICOS DE ACREDITACIÓN	2
3.1. Solicitud y revisión de la solicitud	2
3.2. Investigación de antecedentes de las organizaciones cliente	2
3.3. Alcance de la certificación	3
3.4. Competencia	3
3.5. Competencia del equipo auditor	4
3.6. Auditoría de etapa 1	4
3.7. Auditoría de etapa 2	5
4. PROCESO DE EVALUACIÓN Y DIRECTRICES PARA LAS ENTIDADES DE CERTIFICACIÓN	5
4.1. Grupos de Descripción del Alcance y áreas técnicas relacionadas	5
4.2. Proceso de evaluación	6

Anexo I: Tabla I. Identificación de clústeres y de sectores críticos para certificación de Sistemas de Gestión anti soborno (ISO 37001)

1. GENERAL

La norma internacional de sistema de gestión contra el soborno (ISO 37001), se ajusta a la estructura de alto nivel de ISO para otros sistemas de gestión, siendo posible la acreditación conforme a la norma ISO/IEC 17021-11 de las entidades de certificación (en adelante, EC) que realicen auditorías y certificación según esta norma de sistemas de gestión. Los elementos clave de esta norma de sistemas de gestión han de permitir a las organizaciones:

- evitar, detectar y responder al soborno y cumplir con la legislación anti-soborno aplicable;
- identificar y revisar periódicamente los riesgos relacionados con la amenaza de soborno;
- implantar medidas para minimizar dichos riesgos;
- implantar un sistema de gestión que sea adecuado y proporcionado a los citados riesgos según el tipo y características de la organización; y
- monitorizar los procedimientos anti-soborno de cara a asegurar su continua eficacia.

Se ha publicado además el documento ISO/IEC TS 17021-9, donde se recogen requisitos específicos de competencia para la auditoría y certificación de los sistemas de gestión anti-soborno.

Este documento está basado en el documento CIS 14 Ed.1 “UKAS Guidance for Bodies Offering Certification of Anti-Bribery Management Systems” publicado por UKAS y ha sido elaborado en el seno de Comité Técnico Asesor de Certificación de ENAC.

2. OBJETO Y CAMPO DE APLICACIÓN

Este documento establece criterios específicos de acreditación asociados a la norma en ISO/IEC TS 17021-9, cuando se aplica a los organismos de certificación que pretendan acreditarse según ISO/IEC 17021-11 para certificar ISO 37001 "Sistemas de Gestión contra el soborno - Requisitos con guía de uso".

Los criterios aquí establecidos deben considerarse como complementarios a los establecidos en los documentos PAC-ENAC, CGA-ENAC-CSG y NT 85 que se mantienen como documentos de referencia para el proceso de acreditación.

3. CRITERIOS ESPECÍFICOS DE ACREDITACIÓN

3.1. Solicitud y revisión de la solicitud

Los procesos de solicitud y de revisión de esta por parte de la EC deben asegurar que el grado de conocimiento del potencial cliente es suficiente como para poder realizar una oferta fiable. Podría ser necesario durante la auditoría de etapa 1, revisar la duración de la auditoría de etapa 2 y, por lo tanto, la oferta económica de la auditoría de certificación inicial. La información clave que debe tener en cuenta una EC de cara a la revisión de la solicitud sería similar a "Comprensión de la organización y de su contexto" tal como se establece en la sección 4.1 de ISO 37001.

Para comprender el contexto de negocio, el equipo auditor deberá realizar una investigación independiente relacionada con su cliente, incluido su modelo de negocio y su entorno operativo (ISO/IEC TS 17021-9 cláusula 5.3.2) antes de realizar la visita de la auditoría de etapa 1. El nivel de esta investigación de antecedentes (ver apartado 3.2) puede basarse en una información similar a la que necesita una organización cliente cuando lleva a cabo su proceso de análisis de riesgos "due diligence", (por ejemplo, según lo establecido en el anexo A.10.2 de ISO 37001).

3.2. Investigación de antecedentes de las organizaciones cliente

Si bien se reconoce que una auditoría del sistema de gestión ISO 37001 no implica una investigación en profundidad del cliente, la EC 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.

La EC 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 EC necesite un procedimiento documentado que describa la forma en que se realiza esta investigación independiente.

Algunos factores de los riesgos de soborno que deben ser considerados son:

- el perfil de riesgo del cliente para soportar una evaluación de riesgos de soborno;
- los factores de riesgo socioeconómico y sociopolítico adoptados e implantados dentro de la evaluación del riesgo contra el soborno del cliente;
- las fuentes y agentes de las amenazas, los niveles de motivación y las capacidades de amenaza de cara a confirmar que un cliente ha seleccionado y aplicado los controles apropiados;
- los controles de seguimiento establecidos por el cliente para el análisis de comportamiento y sistemas; y
- el conocimiento de la legislación de prevención del soborno aplicable en los países en que opera el cliente y que puede afectar áreas como la política de regalos y atenciones. Leyes relacionadas en los países en los que actúa.

3.3. Alcance de la certificación

Si la organización cliente de la EC solicita la exclusión de ubicaciones geográficas o actividades concretas (por ejemplo, actividades distintas a ventas, operaciones, proveedores, socios comerciales y mercados existentes), la EC 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.

La EC debe documentar 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 anti-soborno dentro de la entidad legal del cliente.

3.4. Competencia

Las EC deben determinar los criterios de competencia para el personal involucrado en la gestión y la realización de las auditorías, así como para otras actividades del proceso de certificación de sistemas de gestión anti-soborno. Los criterios de competencia se determinarán con respecto a los requisitos de la norma del sistema de gestión anti-soborno, para cada área técnica y para cada función en el proceso de certificación. Los requisitos específicos de competencia en relación a la gestión anti-soborno, se han establecido en la norma ISO/IEC TS 17021-9. El equipo de auditoría debe tener un 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, los cuales pueden variar entre los diferentes Grupos de Descripción del Alcance.

3.5. Competencia del equipo auditor

ISO/IEC 17021-11 requiere que el equipo de auditoría tenga conocimiento de los sectores de negocio del cliente en términos de terminología, prácticas y procesos en el contexto del sistema de gestión anti-soborno. Es necesario conocer al cliente lo suficientemente bien como para comprender sus operaciones de negocio y cómo puede aplicar los requisitos del sistema de gestión. Además, la norma ISO/IEC TS 17021-9 requiere que el equipo auditor tenga conocimientos y habilidades para diseñar y evaluar controles anti-soborno y para investigar los mismos, así como para diseñar o implementar un sistema de gestión similar de *compliance* o de control interno.

Por lo tanto, el equipo de auditoría tendrá que demostrar conocimiento de los riesgos de soborno pertinentes a las actividades de negocio de la organización cliente y a los lugares donde opera, al objeto de emitir juicios globales en relación con la exhaustividad de la evaluación de riesgos del cliente y sobre la idoneidad y eficacia de las medidas preventivas adoptadas.

El equipo auditor debe también tener el conocimiento de la legislación aplicable y de los riesgos de soborno asociados según los países, las regiones y los mercados donde su cliente realiza actividades de negocio (ISO 17021-1 cláusula 7.1.1).

Si una EC planea formar a auditores de otros sistemas de gestión para esta certificación, deberá demostrar cómo 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 sistemas de gestión anti-soborno y los requisitos de ISO 37001.

3.6. Auditoría de etapa 1

La auditoría de etapa 1 tiene el objetivo principal de confirmar la preparación de un cliente para la auditoría, según los objetivos enumerados en la norma ISO/IEC 17021-1.

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 anti-soborno 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 anti-soborno. 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).

3.7. Auditoría de etapa 2

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 anti-soborno 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 anti-soborno 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”. Si una EC ofrece una certificación global para una actividad específica del cliente, la auditoría realizada del sistema de gestión anti-soborno, 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

4. PROCESO DE EVALUACIÓN Y DIRECTRICES PARA LAS ENTIDADES DE CERTIFICACIÓN

La acreditación a las EC de sistemas de gestión anti-soborno según ISO 37001, se llevará a cabo utilizando las normas ISO/IEC 17021-1 e ISO/IEC TS 17021-9 como requisitos de acreditación.

4.1. Grupos de Descripción del Alcance y áreas técnicas relacionadas

ENAC concederá la acreditación utilizando los Grupos de Descripción del Alcance o Cluster, basados en riesgos similares de soborno para sectores del mercado y en los riesgos percibidos y detallados en el Anexo I. Podrían identificarse, si es necesario, áreas geográficas donde la EC declare o no haya podido demostrar ser competente para realizar una auditoría eficaz. La EC deberá demostrar conocimiento y concienciación sobre los riesgos de soborno y los controles asociados, según los Clúster y las localizaciones geográficas dentro de su alcance de acreditación.

La EC puede considerar esos grupos al determinar sus áreas técnicas específicas dentro de cada categoría de alcance. La EC deberá demostrar que conoce los riesgos locales de soborno a través de una evaluación de riesgos predeterminada o de un proceso eficaz para identificar los riesgos durante la etapa de investigación de antecedentes (ver la sección 4.3).

ENAC, por razones de riesgo, podría también decidir no ofrecer acreditación para ciertas zonas geográficas fuera de la UE.

4.2. Proceso de evaluación

Se categorizan los clúster de acuerdo a su riesgo percibido/real de soborno en tres categorías ALTO/MEDIO/BAJO, ver Anexo I. A los efectos de la aplicación del documento de ENAC NT 85 se considera que los códigos incluidos en clúster considerados como de riesgo alto son “críticos” y los incluidos en clúster de riesgo medio y bajo son “no críticos”. Los riesgos asociados a ubicaciones geográficas específicas se tendrán en cuenta países con puntuación inferior a 70 en el Índice de Percepción de la Corrupción de Transparencia Internacional (<https://www.transparency.org/country>).

La edición en vigor de este documento está disponible en www.enac.es. Las organizaciones acreditadas deben asegurarse de que disponen de la edición actualizada.

Puede enviar a ENAC sus puntos de vista y comentarios en relación con este documento, así como sus propuestas de cambio o de mejora para futuras ediciones, en la siguiente dirección (calidad@enac.es) indicando en el asunto el código del documento.

Tabla I. Identificación de clústeres y de sectores críticos para certificación de Sistemas de Gestión anti soborno (ISO 37001)

Clúster técnico	Código IAF	Códigos Nace 2	Categorización del Riesgo
Agricultura, silvicultura y pesca	01	01, 02 y 03	MEDIO
Tecnologías de la información y telecomunicaciones	31 (sólo comunicaciones) y 33	58, 59, 60, 61, 62 y 63	MEDIO
Fabricación ligera y pesada	[3, 4, 5, 6, 7], [12, 14, 15, 17, 18 (excluidas armas), 19, 23 (excluidos equipos médicos)], 20,	10, 11, 12, 13, 14, 15, 16, 17, 18, 20 (excluido 20.51 – explosivos), 22, 23 (excluidos 23.5 y 23.6 hormigón y yeso), 24, 25 (excluido 25.4 – armas) , 26, 27, 28, 29, 30 (excluidos 30.3 y 30.4 – aeronaves y militar), 31, 32 (excluido 32.5 – instrumentos médico y dentales), 33 (excluido 33.16 – reparación de aeronaves y naves espaciales)	MEDIO
Industria aeroespacial, armamentística y defensa	18 (armas), 21 y 36 (relacionados con Defensa)	20.51, 25.4, 30.3, 30.4, 33.16 y 84.22	ALTO
Banca y finanzas. Sector inmobiliario y servicios legales de negocios	[32 y 35 (legal y contable)]	64, 65, 66, 68, 69, 92	ALTO
Construcción y Administración Pública	16, 28 y 36	23.5, 23.6, 41, 42, 43 y 84 (excluido 84.22)	ALTO
Generación y transmisión de energía, minería y refino de petróleo; servicios básicos	02, [10, 11], [24, 25, 26, 27]	05, 06, 07, 08, 09, 19, 35, 36, 37, 38, 39, 46.12	ALTO
Sectores farmacéutico y sanitario	13, 23 (equipos médicos) y 38	21, 32.5, 46.46, 86, 87, 88	ALTO
Transporte y almacenamiento	22, 29 (automóviles), 31 (excluidas comunicaciones)	45, 49, 50, 51, 52, 53	MEDIO
Edición e impresión, servicios sociales y de consumo, educación y servicios de educación e ingeniería	08 (edición), 09 (impresión) 29 (no vehículos y productos farmacéuticos), 30, 34 (servicios de ingeniería), 35 (no legal y contables), 37 (educación), 39	46 (excluido 46.12 – agentes mineros, 46.46 – agentes farmacéuticos), 47 55, 56, 70, 71, 72, 73, 74, 75, 77, 78, 79, 80, 81, 82, 85, 90, 91, 93, 94, 95, 96, 97, 98, 99	BAJO