NORMA TÉCNICA COLOMBIANA

NTC-ISO 21101

2020-11-25

Turismo de aventura. Sistemas de gestión de seguridad. Requisitos

E: Adventure tourism. Safety management systems. Requirements

CORRESPONDENCIA: Esta norma Técnica Colombiana es una adopción idéntica y por traducción (IDT) de la norma ISO 21101:2014 (revisado y confirmado 2019)

DESCRIPTORES: sistemas de gestión; turismo de aventura; turismo; seguridad.

I.C.S.: 03.200;03.080.30

Editada por ICONTEC. Apartado 14237 Bogotá, D.C. - Tel. (571) 6078888

PRÓLOGO

El Instituto Colombiano de Normas Técnicas y Certificación, **ICONTEC**, es el organismo nacional de normalización, según el Decreto 1595 de 2015.

ICONTEC es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el período de Consulta Pública, este último caracterizado por la participación del público en general.

Se llama la atención sobre la posibilidad de que algunos elementos de este documento pueden ser objeto de derechos de patente. ICONTEC no asume la responsabilidad por la identificación de dichas patentes, o por la documentación que se haya aportado que goza de esta protección legal.

El proceso de elaboración de la norma NTC-ISO 21101 fue liderado por el Ministerio de Comercio, Industria y Turismo, con el Fondo de Turismo - FONTUR como contratante del proceso.

La norma NTC-ISO 21101 fue elaborada por el CTN 258 Turismo de Aventura y Buceo y ratificada por el Consejo Directivo de 2020-11-25.

Este documento está sujeto a ser revisado en cualquier momento con el objeto de que responda a las necesidades y exigencias actuales. Se invita a los usuarios de este documento a presentar sus solicitudes de revisión a ICONTEC; sus comentarios serán puestos a consideración del comité técnico responsable del estudio de este tema.

ICONTEC cuenta con un Centro de Información que pone a disposición de los interesados normas internacionales, regionales y nacionales y otros documentos relacionados.

DIRECCIÓN DE NORMALIZACIÓN

CONTENIDO

Página

Página

Página

ANEXOS

INTRODUCCIÓN

0.1 TURISMO DE AVENTURA

El turismo de aventura es una industria mundial cada vez más importante. Ya sea que se realicen con fines comerciales, sin ánimo de lucro o con fines de beneficencia, las actividades de turismo de aventura entrañan un elemento inherente y aceptado de riesgo y desafío. Tomar riesgos conlleva recompensas, pero también peligros. Para maximizar las recompensas, los proveedores de actividades de turismo de aventura deben operar con la mayor seguridad posible.

Esta norma, junto las normas ISO/TR 21102 e ISO 21103, proporcionan una base para que los proveedores de actividades de turismo de aventura planifiquen, comuniquen y ofrezcan actividades de turismo de aventura de la forma más segura posible.

La aplicación eficaz de la presente norma y las normas ISO/TR 21102 e ISO 21103 ayudará a los consumidores a elegir con conocimiento de causa las actividades y los proveedores.

0.2 NORMAS DE TURISMO DE AVENTURA

El propósito de las normas de turismo de aventura es establecer los requisitos mínimos de los sistemas de gestión de seguridad y la comunicación con los participantes. Son entidades independientes ya que se aplican a diferentes aspectos del turismo de aventura.

- esta norma específica cómo la organización de turismo de aventura gestiona sus operaciones en términos de seguridad;
- la norma ISO/TR 21102 proporciona datos sobre la competencia mínima de los líderes de actividades de turismo de aventura;
- la norma ISO 21103 especifica la información mínima que debe comunicarse a los participantes actuales y potenciales antes, durante y después de la actividad para garantizar la seguridad.

0.3 PROPÓSITO DE ESTA NORMA

El propósito de esta norma es establecer los requisitos mínimos para un sistema de gestión de seguridad de proveedores de actividades de turismo de aventura.

El proceso de gestión del riesgo es parte integral de un sistema de gestión de la seguridad. Un sistema de gestión de seguridad proporciona el marco para la mejora continua y contribuye a la realización de actividades de turismo de aventura seguras.

El enfoque del sistema de gestión de seguridad motiva a los proveedores a analizar sus actividades de turismo de aventura, comprender los requisitos de los participantes, definir los procesos que garanticen seguridad y mantener estos procesos bajo control.

TURISMO DE AVENTURA.
SISTEMAS DE GESTIÓN DE SEGURIDAD.
REQUISITOS

1. OBJETO Y CAMPO DE APLICACIÓN

La presente norma establece los requisitos para un sistema de gestión de seguridad de proveedores de actividades de turismo de aventura.

Un proveedor puede utilizar esta norma para lo siguiente:

a) mejorar el cumplimiento de la seguridad;

b) satisfacer las expectativas de seguridad de los participantes y el personal;

c) demostrar prácticas seguras;

d) apoyar el cumplimiento de requisitos legales aplicables.

Puede ser utilizada por proveedores de todo tipo y tamaño, que operen en diferentes entornos geográficos, culturales y sociales.

2. REFERENCIAS NORMATIVAS

No hay referencias normativas

3. TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento, se aplican los siguientes términos y definiciones.

3.1 organización (*organization*). Persona o grupo de personas que tienen sus propias funciones y responsabilidades, autoridades y relaciones para el logro de sus objetivos (3.9)

Nota 1 a la entrada El concepto de organización incluye, entre otros, un trabajador independiente, compañía, corporación, firma, empresa, autoridad, sociedad, organización benéfica o institución, o una parte o combinación de éstas, ya estén constituidas o no y sean públicas o privadas.

3.2 parte interesada (*interested party*). Persona u organización (3.1) que puede afectar, verse afectada por, o percibirse como afectada por una decisión o actividad.

3.3 requisito (*requirement*). Necesidad o expectativa establecida, generalmente implícita u obligatoria.

Nota 1 a la entrada "Generalmente implícita" significa que es habitual o práctica común para la organización y las partes interesadas que la necesidad o expectativa bajo consideración está implícita.

Nota 2 a la entrada Un requisito especificado es el que está declarado, por ejemplo, en información documentada.

3.4 sistema de gestión (*management system*). Conjunto de elementos de una organización (3.1) que están interrelacionados o que interactúan para establecer políticas (3.7) y objetivos (3.9) y procesos (3.13) para lograr estos objetivos.

Nota 1 a la entrada Un sistema de gestión puede abordar una única disciplina o varias.

Nota 2 a la entrada Los elementos del sistema incluyen la estructura de la organización, los roles y responsabilidades, la planificación, la operación, etc.

Nota 3 a la entrada El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas, secciones específicas e identificadas o una o más funciones en todo un grupo de organizaciones.

3.5 alta dirección (*top management*). Persona o grupo de personas que dirige y controla una organización (3.1) al más alto nivel.

Nota 1 a la entrada La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la organización.

Nota 2 a la entrada Si el alcance del sistema de gestión (3.4) comprende solo una parte de una organización, entonces "alta dirección" se refiere a quienes dirigen y controlan esa parte de la organización.

3.6 eficacia (*effectiveness*). Medida en que se realizan las actividades planificadas y se logran los resultados previstos.

3.7 política (*policy*). Intenciones y dirección de una organización (3.1), como las expresa formalmente su alta dirección (3.5).

3.8 política de seguridad (*safety policy*). Política de una organización (3.1) con respecto a su desempeño en materia de seguridad.

Nota 1 a la entrada La política de seguridad proporciona una estructura para la acción y la definición de sus objetivos de seguridad.

3.9 objetivo (*objective*). Resultado a lograr.

Nota 1 a la entrada Un objetivo puede ser estratégico, táctico u operacional.

Nota 2 a la entrada Los objetivos pueden estar relacionados con diferentes disciplinas (como las metas financieras, de salud y seguridad, y ambientales) y pueden aplicarse a diferentes niveles (como el estratégico, el organizacional en general, el de proyectos, el de productos y el de procesos (3.13)).

Nota 3 a la entrada Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operacional, un objetivo de seguridad de turismo de aventura, o mediante el uso de otros términos con un significado similar (por ejemplo, finalidad, meta u objeto).

Nota 4 a la entrada En el contexto de los sistemas de gestión de la seguridad de turismo de aventura, la organización establece objetivos de seguridad para el turismo de aventura, en consonancia con la política de seguridad de turismo de aventura, a fin de lograr resultados específicos.

3.10 riesgo (*risk*). Efecto de la incertidumbre.

Nota 1 a la entrada Un efecto es una desviación de aquello que se espera — ya sea positivo o negativo.

Nota 2 a la entrada La incertidumbre es el estado, incluso parcial, de la deficiencia de información relacionada con un acontecimiento, su comprensión o conocimiento, su consecuencia o su posibilidad.

Nota 3 a la entrada El riesgo suele caracterizarse por referencia a los posibles eventos (3.38) y las consecuencias (3.39), o una combinación de éstos.

Nota 4 a la entrada El riesgo suele expresarse en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la posibilidad (3.41) asociada de que ocurra.

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

3.12 información documentada (*documented information*). Información que una organización (3.1) tiene que controlar y mantener, y el medio que la contiene.

Nota 1 a la entrada La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

Nota 2 a la entrada La información documentada puede hacer referencia a:

- el sistema de gestión (3.4), incluidos los procesos (3.13) relacionados;
- información creada para la operación de la organización (documentación);
- la evidencia de los resultados alcanzados (registros).

3.13 proceso (*process*). Conjunto de actividades interrelacionadas o que interactúan, que transforman las entradas en salidas.

3.14 desempeño (*performance*). Resultado medible.

Nota 1 a la entrada El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada El desempeño se puede relacionar con la gestión de actividades, procesos (3.13), productos (incluidos servicios), sistemas u organizaciones (3.1).

3.15 contratar externamente (*outsource*). <verbo>**.** Establecer un acuerdo mediante el cual una organización (3.1) externa realiza parte de una función o proceso (3.13) de una organización.

Nota 1 a la entrada Una organización externa está fuera del alcance del sistema de gestión (3.4), aunque la función o proceso contratado externamente forme parte del alcance.

3.16 seguimiento (*monitoring*). Determinación del estado de un sistema, un proceso (3.13) o una actividad.

Nota 1 a la entrada Una organización externa está fuera del alcance del sistema de gestión (3.4), aunque la función o proceso contratado externamente forme parte del alcance.

3.16 seguimiento (*monitoring*). Determinación del estado de un sistema, un proceso (3.13) o una actividad.

Nota 1 a la entrada Para determinar el estado puede ser necesario verificar, supervisar u observar de forma crítica.

3.17 medición (*measurement*). Proceso (3.13) para determinar un valor.

3.18 auditoría *(audit*). Proceso (3.13) sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

Nota 1 a la entrada Una auditoría puede ser interna (de primera parte) o externa (de segunda parte o terceros), y puede ser una auditoría combinada (que combina dos o más disciplinas).

Nota 2 a la entrada En la norma ISO 19011 se define "evidencia de auditoría" y "criterios de auditoría".

3.19 conformidad (*conformity*). Cumplimiento de un requisito (3.3).

3.20 no conformidad (*nonconformity*). Incumplimiento de un requisito (3.3).

3.21 corrección (*correction*). Acción para eliminar una no conformidad (3.20) detectada.

3.22 acción correctiva (*corrective action*). Acción para eliminar la causa de una no conformidad (3.20) y evitar que vuelva a ocurrir.

3.23 mejora continua (*continual improvement).* Actividad recurrente para mejorar el desempeño (3.14).

3.24 incidente (*incident*). Evento (3.38) que conduce a un accidente o tiene el potencial para conducir a un accidente (3.25).

Nota 1 a la entrada El término “incidente” incluye los “casi accidentes” y los “accidentes (3.25)”.

Nota 2 a la entrada Un incidente en el que no se produce ninguna enfermedad, lesión, daño o cualquier otra pérdida se denomina también "casi accidente".

3.25 accidente (*accident).* Incidente (3.24) que ocasiona muerte, enfermedad lesión u otro perjuicio.

3.26 peligro (*hazard*). Fuente de daño potencial.

Nota 1 a la entrada Un peligro puede ser una fuente de riesgo.

[FUENTE: Guía ISO 73:2009, 3.5.1.4]

3.27 identificación del peligro (*hazard identification*). Proceso de reconocimiento de la existencia de un peligro (3.26) y definición de sus características.

3.28 identificación del riesgo (*risk identification*). Proceso de hallar, reconocer y describir riesgos (3.10).

Nota 1 a la entrada La identificación del riesgo implica la identificación de las fuentes de riesgo, los eventos (3.38), sus causas y sus posibles consecuencias (3.39).

Nota 2 a la entrada La identificación de los riesgos puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de las partes interesadas (3.2).

3.29 evaluación del riesgo (*risk assessment*). Proceso general de identificación del riesgo (3.28), análisis del riesgo (3.30) y valoración del riesgo (3.32).

[FUENTE: Guía ISO 73:2009, 3.4.1]

3.30 análisis del riesgo (*risk analysis*). Proceso para comprender la naturaleza del riesgo (3.10) y determinar el nivel de riesgo (3.31).

Nota 1 a la entrada El análisis del riesgo proporciona la base para la evaluación del riesgo (3.32) y las decisiones sobre el tratamiento del riesgo (3.33).

Nota 2 a la entrada El análisis del riesgo incluye la estimación del riesgo

[FUENTE: Guía ISO 73:2009, 3.6.1]

3.31 nivel de riesgo (*level of risk*). Magnitud de un riesgo (3.10) o combinación de riesgos, expresada en términos de la combinación de consecuencias (3.39) y su posibilidad (3.41).

[FUENTE: Guía ISO 73:2009, 3.6.1.8]

3.32 valoración del riesgo (*risk evaluation).* Proceso de comparación de los resultados del análisis del riesgo (3.30) con los criterios de riesgo para determinar si el riesgo (3.10) y/o su magnitud es aceptable o tolerable.

Nota 1 a la entrada La valoración del riesgo ayuda a tomar decisiones sobre el tratamiento del riesgo (3.33).

[FUENTE: Guía ISO 73:2009, 3.7.1]

3.33 tratamiento del riesgo (*risk treatment*). Proceso de modificar el riesgo (3.10).

Nota 1 a la entrada El tratamiento del riesgo puede incluir:

- evitar el riesgo decidiendo no iniciar o continuar con la actividad que da origen al riesgo;
- tomar o aumentar el riesgo con el fin de buscar una oportunidad;
- eliminar la fuente de riesgo;
- cambiar la posibilidad (3.41);
- cambiar las consecuencias (3.39);
- compartir el riesgo con otra u otras partes, incluyendo contratos y financiación del riesgo; y
- retención del riesgo por una decisión informada.

Nota 2 a la entrada Los tratamientos del riesgo que se ocupan de las consecuencias negativas se denominan a veces "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

Nota 3 a la entrada El tratamiento del riesgo puede crear riesgos nuevos o modificar los existentes.

[FUENTE: Guía ISO 73:2009, 3.8.1]

3.34 seguridad (*safety*). Estado en el que el riesgo (3.10) de daño (a las personas) o perjuicio se limita a un nivel aceptable.

3.35 actividad de turismo de aventura (*adventure tourism activity*)[1]. Actividad de aventura con fines turísticos que implica un grado de instrucción o liderazgo y un elemento de riesgo (3.10) deliberadamente aceptado.

Nota 1 a la entrada: Un elemento de riesgo aceptado significa que el participante tiene una comprensión mínima del riesgo que implica.

Nota 2 a la entrada: La actividad de turismo de aventura está asociada al turismo de naturaleza

3.36 proveedor de actividad de turismo de aventura (*adventure tourism activity provider*). Individuo u organización (3.1) que es responsable en general de todos los aspectos de la provisión de actividades de turismo de aventura (3.35).

Nota 1 a la entrada: Las actividades de turismo de aventura pueden ser provistas de forma gratuita o con pago a cambio.

3.37 participante (*participant*). Persona que hace parte de una actividad de turismo de aventura (3.35) sin ser miembro del equipo de liderazgo.

Nota 1 a la entrada: A un participante también se le puede denominar "cliente", "usuario" o similar.

Nota 2 a la entrada: El equipo de liderazgo está compuesto de varios líderes.

3.38 evento (*event*). Ocurrencia o cambio de un conjunto de circunstancias particulares.

Nota 1 a la entrada: Un evento puede estar constituido por una o más ocurrencias y puede tener varias causas.

Nota 2 a la entrada: Un evento puede consistir en algo que no está sucediendo.

Nota 3 a la entrada: Un evento puede denominarse a veces "incidente (3.24)" o "accidente (3.25)".

Nota 4 a la entrada: Un evento sin consecuencias (3.39) también puede denominarse "cuasiincidente", "incidente (3.24)", o "casi-incidente".

[FUENTE: Guía ISO 73:2009, 3.5.1.3]

3.39 consecuencia (*consequence*). Resultado de un evento (3.38) que afecta los objetivos (3.9).

Nota 1 a la entrada: Un evento puede conducir a una serie de consecuencias.

Nota 2 a la entrada: Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos sobre los objetivos.

Nota 3 a la entrada: Las consecuencias pueden expresarse cualitativa o cuantitativamente.

Nota 4 a la entrada: Las consecuencias iniciales pueden tener repercusiones.

[FUENTE: Guía ISO 73:2009, 3.6.1.3]

[1] Para Colombia, la actividad de turismo de aventura está asociada al turismo de naturaleza

3.40 probabilidad (*probability*). Medida de la oportunidad de ocurrencia expresada como un número entre 0 y 1, donde 0 es la imposibilidad y 1 es la certeza absoluta.

Nota 1 a la entrada Véanse las secciones 3.41 y la NOTA 2.

[FUENTE: Guía ISO 73:2009, 3.6.1.4]

3.41 posibilidad (*likelihood*). Oportunidad de que algo ocurra.

Nota 1 a la entrada En la terminología de gestión del riesgo (3.10), la palabra "posibilidad" se utiliza para referirse a la oportunidad de que algo suceda, ya sea definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito con términos generales o de forma matemática [tal como una probabilidad (3.40) o una frecuencia en un período de tiempo determinado].

Nota 2 a la entrada El término inglés "*likelihood*" (posibilidad) no tiene un equivalente directo en algunos idiomas; en cambio, se suele utilizar el equivalente del término "*probability*" (probabilidad). Sin embargo, en inglés, "*probability*" (probabilidad) suele interpretarse en sentido estricto como un término matemático. Por consiguiente, en la terminología de gestión de riesgos, la palabra "posibilidad" (*likelihood*) se utiliza con la intención de que tenga la misma interpretación amplia que el término "probabilidad" (*probability*) tiene en muchos idiomas distintos del inglés.

[FUENTE: Guía ISO 73:2009, 3.6.1.1]

3.42 procedimiento (*procedure*). Forma específica de llevar a cabo una actividad o un proceso (3.13).

Nota 1 a la entrada Los procedimientos pueden estar documentados o no.

Nota 2 a la entrada Cuando se documenta un procedimiento, se suele utilizar el término "procedimiento escrito" o "procedimiento documentado". El documento que contiene un procedimiento puede llamarse "documento de procedimiento".

[FUENTE: ISO 9000:2005, 3.4.5]

3.43 emergencia (emergency). situación grave que requiere una acción inmediata.

3.44 tercero proveedor (*third party provider*). Organización externa (3.1) o individuo que presta servicios al proveedor de actividades de turismo de aventura (3.36).

4. CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y de su contexto

La organización debe determinar los asuntos externos e internos que son pertinentes para su propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de seguridad de turismo de aventura.

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

- las partes interesadas que son relevantes para el sistema de gestión de la seguridad de turismo de aventura, y

- los requisitos de estas partes interesadas.

4.3 Determinación del alcance del sistema de gestión de seguridad de turismo de aventura

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

Al determinar este alcance, la organización debe considerar:

- los asuntos externos e internos mencionados en el numeral 4.1; y

- los requisitos a los que se hace referencia en el numeral 4.2.

El alcance debe estar disponible como información documentada.

4.4 Sistema de gestión de seguridad de turismo de aventura

La organización debe establecer, aplicar, mantener y mejorar continuamente un sistema de gestión de seguridad de turismo de aventura, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de la presente Norma.

5 LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe demostrar su liderazgo y compromiso con respecto al sistema de gestión de seguridad de turismo de aventura mediante las siguientes acciones:

a) asegurar que se establezcan la política de seguridad de turismo de aventura y los objetivos de seguridad y que sean compatibles con la dirección estratégica de la organización;

b) asegurarse de la integración de los requisitos del sistema de gestión de la seguridad de turismo de aventura en los procesos empresariales de la organización;

c) asegurar la disponibilidad de los recursos necesarios para el sistema de gestión de la seguridad de turismo de aventura;

d) comunicar la importancia de una gestión eficaz de la seguridad y de ajustarse a los requisitos del sistema de gestión de la seguridad de turismo de aventura;

e) asegurar que el sistema de gestión de la seguridad de turismo de aventura logre los resultados previstos;

f) dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de turismo de aventura;

g) promover la mejora continua;

h) apoyar a otras funciones de gestión pertinentes para demostrar su liderazgo en sus esferas de responsabilidad.

NOTA La referencia a actividades "empresariales" en la presente Norma puede interpretarse en sentido amplio como aquellas actividades que son fundamentales para los fines de la existencia de la organización.

5.2 Política

La alta dirección debe establecer una política de seguridad de turismo de aventura que:

a) sea apropiada para el propósito de la organización;

b) proporcione el marco para establecer los objetivos de seguridad de turismo de aventura;

c) incluya el compromiso de satisfacer los requisitos aplicables; e

d) incluya el compromiso de mejorar continuamente el sistema de gestión de la seguridad de turismo de aventura.

NOTA Los requisitos aplicables en este contexto incluyen los legales y normativos.

La política de seguridad de turismo de aventura debe:

- estar disponible como información documentada;
- comunicarse dentro de la organización;
- estar disponible para las partes interesadas, según sea apropiado.

5.3 Roles, responsabilidades y autoridades en la organización

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

La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de la seguridad de turismo de aventura se ajuste a los requisitos de esta norma;

b) informar a la alta dirección sobre el funcionamiento del sistema de gestión de la seguridad del turismo de aventura.

NOTA Los roles pertinentes son aquellos que tienen impacto en la seguridad, incluyendo los líderes de actividades de turismo de aventura[2].

[2] Para definición de “líder” puede consultarse las definiciones dadas en la ISO 21102 e ISO 21103

6. PLANIFICACIÓN

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 Generalidades

Al planificar el sistema de gestión de seguridad de turismo de aventura, la organización debe considerar los asuntos mencionados en el numeral 4.1 y los requisitos mencionados en el numeral 4.2 y determinar los riesgos y oportunidades que deben abordarse para:

- asegurar que el sistema de gestión de la seguridad de turismo de aventura pueda lograr los resultados previstos;
- evitar o reducir efectos indeseados;
- lograr mejora continua.

La organización debe planificar:

a) acciones para abordar estos riesgos y oportunidades y

b) cómo:
   - integrar e implementar las acciones en sus procesos del sistema de gestión de la seguridad de turismo de aventura;
   - evaluar la eficacia de estas acciones.

6.1.2 Proceso de gestión del riesgo de turismo de aventura

La organización debe establecer y aplicar un proceso sistemático de gestión de riesgos para sus actividades de turismo de aventura.

El proceso de gestión del riesgo debe establecer el contexto de las actividades, evaluar los riesgos, abordarlos y debe estar documentado.

El proceso de gestión de riesgos debe ser parte integral del sistema de gestión de la seguridad de turismo de aventura de la organización. En el Anexo A se presentan detalles adicionales.

6.1.3 Requisitos legales

La organización debe establecer, aplicar y mantener procedimientos para identificar requisitos legales y otros requisitos pertinentes, y debe cumplirlos.

La organización debe comunicar la información pertinente sobre los requisitos legales y otros requisitos a sus empleados, proveedores, participantes en actividades y otras partes interesadas.

6.2 Objetivos de seguridad de turismo de aventura y planificación para lograrlos

La organización debe establecer objetivos de seguridad para el turismo de aventura en las funciones y niveles pertinentes.
Los objetivos de seguridad deben:

a) ser coherentes con la política de seguridad;

b) ser medibles (si es posible);

c) tener en cuenta los requisitos aplicables;

d) someterse a seguimiento;

e) comunicarse y

f) actualizarse según sea apropiado.

Cuando se establezcan los objetivos de seguridad, la alta dirección debería tener en cuenta:

a) los beneficios potenciales;

b) peligros y riesgos;

c) equipos técnicos y aplicación;

d) métodos de comunicación;

e) los requisitos financieros, operacionales y comerciales;

f) los puntos de vista de las partes interesadas.

La organización debe retener información documentada sobre los objetivos de seguridad de turismo de aventura.

Al planificar cómo lograr sus objetivos de seguridad en el turismo de aventura, la organización debe determinar:

- qué se hará;
- qué recursos se requerirán;
- quién será responsable;
- cuándo se completará;
- cómo se evaluarán los resultados.

Se deben revisar regularmente los planes para alcanzar los objetivos de seguridad de turismo de aventura. Se deben actualizar para hacer frente a los cambios en las actividades o las condiciones operacionales.

La documentación sobre el tratamiento de los riesgos debe considerarse parte de la planificación para alcanzar los objetivos de seguridad de turismo de aventura.

7. APOYO

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del sistema de gestión de la seguridad de turismo de aventura.

7.2 Competencia

ISO 21102: competencias comunes (incluyendo habilidades, conocimientos y actitudes) de los líderes para dirigir

La organización debe:

a) determinar la competencia necesaria de la(s) persona(s) que realiza(n) un trabajo bajo su control que afecte su cumplimiento de la seguridad en el turismo de aventura;

b) asegurarse de que esas personas sean competentes[3] sobre la base de una educación, formación o experiencia apropiadas;

c) cuando proceda, emprender acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones emprendidas; y

d) retener la información documentada apropiada como evidencia de su competencia.

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

Se deberían utilizar calificaciones reconocidas a nivel nacional o internacional cuando sea pertinente.

7.3 Toma de conciencia

Las personas que realicen trabajos bajo el control de la organización deben estar al tanto de:

a) a política de seguridad de turismo de aventura;

b) su contribución a la eficacia del sistema de gestión de la seguridad de turismo de aventura, incluidos los beneficios de la mejora de la seguridad;

c) las consecuencias de no cumplir los requisitos del sistema de gestión de seguridad de turismo de aventura.

[3] Para definición de “persona competente” pueden consultarse las definiciones dadas en la ISO 21102 e ISO 21103.

Las personas con funciones relacionadas con la seguridad demostrarán su compromiso con la mejora continua del desempeño del sistema de gestión de seguridad de turismo de aventura.

7.4 Comunicación

7.4.1 Generalidades

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes para el sistema de gestión de la seguridad de turismo de aventura, incluyendo:

a) sobre qué comunicará;

b) cuándo comunicar;

c) con quien comunicarse;

d) cómo comunicarse.

7.4.2 Comunicación y consulta con las personas que participan en la prestación de actividades de turismo de aventura

La organización debe establecer un proceso de comunicación y consulta con el personal y otras personas que participan en la prestación de actividades de turismo de aventura para asegurarse de que:

a) se comprometen con la elaboración y la revisión de las políticas y procedimientos de gestión de la seguridad;

b) sean consultados cuando haya cambios que afecten su seguridad en la realización de actividades de turismo de aventura;

c) estén representados en asuntos de seguridad; y

d) estén informados acerca de quién los representa en asuntos de seguridad y quién representa a la alta dirección.

Se debe documentar este proceso.

7.4.3 Comunicación y consulta con los participantes

La organización debe establecer un proceso de comunicación y consulta con los participantes para asegurar que:

- la información sobre seguridad se comunica a los participantes; y

- se pide a los participantes que proporcionen a la organización información que pueda afectar a la gestión de la seguridad.

Se debe documentar este proceso.

NOTA En la norma ISO 21103 se encuentra mayor orientación.

7.5 Información documentada

7.5.1 Generalidades

El sistema de gestión de la seguridad de turismo de aventura de la organización debe incluir:

a) la información documentada requerida por esta norma;

b) la información documentada que la organización determine como necesaria para la eficacia del sistema de gestión de la seguridad de turismo de aventura.

NOTA 1 El alcance de la información documentada para un sistema de gestión de la seguridad de turismo de aventura puede diferir de una organización a otra debido a:

- el tamaño de la organización y su tipo de actividades, procesos, productos y servicios,
- la complejidad de los procesos y sus interacciones, y
- la competencia de las personas.

La organización debe establecer y mantener información documentada para:

- describir los principales elementos del sistema de gestión de seguridad de turismo de aventura y la interacción entre ellos; y
- orientación sobre la información documentada relacionada.

NOTA 2 La información documentada incluye procedimientos y registros documentados.

7.5.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe asegurar la apropiada:

a) identificación y descripción (por ejemplo, un título, una fecha, un autor o un número de referencia);

b) el formato (por ejemplo, el idioma, la versión de software, los gráficos) y los medios (por ejemplo, papel, electrónico);

c) examen y aprobación de la idoneidad y la adecuación.

Control de la información documentada

La información documentada requerida por el sistema de gestión de seguridad de turismo de aventura y por esta norma debe controlarse para asegurar que:

- está disponible y es adecuada para los usuarios, donde y cuando se necesita;
- está protegida adecuadamente (por ejemplo, contra la pérdida de confidencialidad, el uso indebido o la pérdida de integridad).

Para el control de la información documentada, la organización debe ocuparse de las siguientes actividades, según proceda:

a) distribución, acceso, recuperación y utilización;

b) almacenamiento y conservación, incluida la preservación de la legibilidad;

c) el control de los cambios (por ejemplo, el control de versiones);

d) retención y disposición.

La información documentada de origen externo que la organización determine que es necesaria para la planificación y el funcionamiento del sistema de gestión de la seguridad de turismo de aventura debe estar identificada según corresponda, y se debe controlar.

NOTA El acceso implica una decisión sobre el permiso para ver la información documentada solamente, o el permiso y la autoridad para ver y cambiar la información documentada, etc.

Las condiciones de retención deben ser coherentes con el sistema de gestión de seguridad de turismo de aventura de la organización y con cualquier obligación contractual, legal o de otro tipo. Los términos de retención deben estar documentados.

8. OPERACIÓN

8.1 Planificación y control operacional

La organización debe planificar, aplicar y controlar los procesos necesarios para cumplir los requisitos, y para poner en práctica las acciones determinadas en el numeral 6.1, de la siguiente forma:

- estableciendo criterios para los procesos;

- aplicando el control de los procesos de acuerdo con los criterios;

- manteniendo la información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo previsto.

La organización debe controlar los cambios planificados y examinar las consecuencias de los cambios no intencionados, adoptando medidas para mitigar cualquier efecto adverso, según sea necesario.

La organización se debe asegurar de que se controlen los procesos subcontratados.

La organización debe desarrollar e implementar planes, incluyendo planes alternativos, para cumplir con los objetivos de seguridad y tratar los riesgos identificados en el numeral 6.2.

La organización debe planificar las actividades para asegurar que sean ejecutadas eficazmente por:

a) establecer y mantener procedimientos documentados para la realización de actividades de turismo de aventura, cuando su ausencia pueda causar una desviación de la política y los

objetivos de seguridad; estos procedimientos deben incluir medidas de prevención y seguridad para los participantes y el personal;

b) establecer y mantener procedimientos relacionados con bienes, equipos y servicios utilizados en la prestación de actividades de turismo de aventura que podrían afectar la seguridad;

c) definir y documentar la competencia mínima requerida de los participantes;

d) asegurarse de que los participantes tengan la competencia mínima necesaria para realizar la actividad con seguridad.

8.2 Preparación y respuesta ante emergencias

La organización debe identificar las posibles situaciones de emergencia y sus repercusiones, y establecer y mantener planes y procedimientos de respuesta.

La organización se debe asegurar de que se disponga de los servicios apropiados, las personas competentes u otros recursos para aplicar los planes y procedimientos de respuesta a las emergencias.

La organización debe revisar sus planes y procedimientos de respuesta de emergencia.

La organización debe disponer de un procedimiento para recabar de cada participante la siguiente información mínima:

a) datos de identificación (por ejemplo, número de identificación, nombre completo);

b) datos de contacto en caso de emergencia (incluidos el nombre y los medios de contacto);

c) asistencia especia requerida;

d) la salud y las condiciones médicas.

La organización debe reunir, almacenar y utilizar los datos personales de acuerdo con los reglamentos y requisitos aplicables.

La organización debe poner a prueba periódicamente sus procedimientos de respuesta a las emergencias. Los resultados de la prueba serán documentados.

Se debe informar a los participantes de los planes de respuesta de emergencia antes de que comience la actividad.

8.3 Gestión de incidentes

La organización debe establecer y mantener procedimientos para definir las responsabilidades y la autoridad para:

- tratar, informar e investigar los incidentes;

- adoptar medidas a fin de reducir las consecuencias derivadas de los incidentes;

La documentación del incidente debe incluir, como mínimo, la siguiente información:

a) actividad;

b) fecha y hora;

c) ubicación;

d) las personas involucradas, como los participantes y el personal;

e) descripción de las condiciones ambientales, el equipo y las acciones o circunstancias particulares;

f) las probables causas y factores contribuyentes;

g) la respuesta, incluido cualquier tratamiento médico;

h) consecuencias

i) medidas correctivas;

j) fuente de la información.

La organización debe tener un procedimiento para registrar los incidentes.

NOTA El registro y análisis de los incidentes ayuda a prevenir futuros incidentes, a evaluar la eficacia de un sistema de gestión de la seguridad de turismo de aventura y a controlar los riesgos.

9. EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

- qué necesita ser monitoreado y medido;
- los métodos de seguimiento, medición, análisis y evaluación, según proceda, para asegurarse de resultados válidos;
- cuándo se debe realizar el control y la medición;
- cuándo se deben analizar y evaluar los resultados del seguimiento y la medición;
- cómo se deben documentar los resultados del seguimiento, la medición, el análisis y la evaluación.

El seguimiento y la medición deben asegurar:

a) la conformidad con los requisitos de los programas de gestión de la seguridad y los requisitos legales aplicables;

b) la consideración de los incidentes y otros datos históricos;

c) el examen de las experiencias de los participantes y su retroalimentación.

La organización debe retener la información documentada apropiada como prueba de los resultados.

La organización debe evaluar el desempeño en materia de seguridad y la eficacia de los resultados del sistema de gestión de seguridad de turismo de aventura.

9.2 Auditoría interna

La organización debe llevar a cabo auditorías internas a intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de turismo de aventura:

- es conforme con:

- los propios requisitos de la organización para su sistema de gestión de seguridad de turismo de aventura;

- los requisitos de esta norma;

- se aplica y mantiene eficazmente.

La organización debe:

a) planificar, establecer, ejecutar y mantener un programa o programas de auditoría (incluida la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la presentación de informes), en los que se tendrá en cuenta la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;

b) definir los criterios y el alcance de cada auditoría;

c) seleccionar a los auditores y realizar auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría;

d) asegurarse de que los resultados de las auditorías se comuniquen a la administración pertinente; y

e) retener la información documentada como evidencia de la aplicación del programa de auditoría y de los resultados de esta.

El programa de auditoría de la organización debe tener en cuenta los resultados de las evaluaciones de los riesgos (véase el numeral 6.1.2) realizadas sobre las actividades de la organización y los resultados de auditorías anteriores.

9.3 Revisión por la dirección

La alta dirección debe revisar el sistema de gestión de seguridad de turismo de aventura de la organización, a intervalos planificados, para asegurarse de su continua idoneidad, adecuación y eficacia.

La revisión por la dirección debe incluir la consideración de:

a) el estado de las acciones de las revisiones por la dirección anteriores;

b) los cambios en los asuntos externos e internos que son pertinentes para el sistema de gestión de la seguridad de turismo de aventura;

c) información sobre el desempeño en materia de seguridad de turismo de aventura, incluidas las tendencias en:

   1) las no conformidades y las medidas correctivas;

   2) los resultados del seguimiento y la medición; y

   3) los resultados de la auditoría;

d) oportunidades de mejora continua.

Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con las oportunidades de mejora continua y la necesidad de introducir cambios en el sistema de gestión de la seguridad de turismo de aventura.

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

10 MEJORA

10.1 No conformidad y acción correctiva

Cuando se produzca una no conformidad, la organización debe:

a) reaccionar a la no conformidad y, según proceda:

   1) emprender acciones para controlarla y corregirla; y

   2) tratar con las consecuencias;

b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, a fin de que no vuelva a producirse o se produzca en otro lugar, mediante:

   1) revisar la no conformidad;

   2) determinar las causas de la no conformidad; y

3) determinar si existen, o podrían ocurrir, no conformidades similares;

c) implementar cualquier acción necesaria;

d) revisar la eficacia de toda acción correctiva emprendida; y

e) realizar cambios en el sistema de gestión de la seguridad de turismo de aventura, si es necesario.

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

La organización debe retener la información documentada apropiada como evidencia de:

- la naturaleza de las no conformidades y las acciones posteriores adoptadas, y
- los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del sistema de gestión de seguridad de turismo de aventura.

ANEXO A
(Normativo)

PROCESO DE GESTIÓN DEL RIESGO DE TURISMO DE AVENTURA

A.1 GENERALIDADES

Este anexo se relaciona con el numeral 6.1.2, en el que se esbozan tres etapas del proceso de gestión del riesgo para el turismo de aventura:

a) establecer el contexto;

b) evaluación del riesgo

c) tratamiento del riesgo

A.2 ESTABLECIMIENTO DEL CONTEXTO

La organización debe establecer el contexto de cada actividad de turismo de aventura.

Se debe establecer el contexto determinando los objetivos, el alcance y los parámetros de gestión del riesgo de cada actividad.

La organización debe definir:

a) la actividad de turismo de aventura;

b) el alcance de la actividad, como los lugares, la duración y todas las actividades dentro de la actividad;

c) los objetivos de la gestión del riesgo de la actividad;

d) los límites e interfaces con otras actividades o sistemas de gestión de la seguridad;

e) las metodologías de evaluación del riesgo;

f) los criterios de evaluación del riesgo (incluido el nivel de riesgo aceptable) y sus razones.

NOTA Al establecer el contexto de las actividades se puede incluir lo relativo al transporte, el alojamiento, el medio ambiente y los riesgos médicos o culturales.

A.3 EVALUACIÓN DEL RIESGO

La evaluación del riesgo consta de tres pasos.

a) Identificación del riesgo

La organización debe establecer y mantener un proceso sistemático y estructurado para la identificación continua de riesgos para sus actividades de turismo de aventura.

Los procedimientos de identificación de riesgos deben incluir:

- actividades rutinarias y no rutinarias;
- la competencia del participante;
- actividades supervisadas y no supervisadas, y sitios de actividad;
- actividades de todo el personal (incluidos los subcontratistas, los participantes y los visitantes) que tienen acceso a los lugares de trabajo y a los sitios de actividades de turismo de aventura;
- instalaciones, ropa y equipo utilizados en las actividades de turismo de aventura proporcionados por la organización, los participantes y terceros.

La metodología de la identificación del riesgo debe:

- involucrar a los líderes y otras partes interesadas;
- ser coherente con la experiencia operacional;
- seguir la práctica actual, aceptada para el turismo de aventura.

b) Análisis del riesgo

La organización debe analizar el riesgo considerando las causas y las fuentes del mismo, sus consecuencias positivas y negativas y la probabilidad de que esas consecuencias se produzcan. Se tendrán en cuenta los controles existentes y su eficacia.

c) Evaluación del riesgo:

La organización debe evaluar los riesgos contra los criterios de evaluación del riesgo e identificar los que requieren tratamiento.

A.4 TRATAMIENTO DEL RIESGO

La organización debe establecer, aplicar y mantener un proceso de tratamiento de riesgos.

La organización debe identificar las responsabilidades, los plazos, los resultados previstos, los recursos, las medidas de desempeño y los procesos de revisión para el tratamiento de los riesgos.

NOTA En la NTC-ISO 31000 se encuentra información adicional sobre los procesos de gestión del riesgo. La intención de la NTC-ISO 31000 es armonizar los procesos de gestión del riesgo en las normas existentes y futuras.

ANEXO B
(Informativo)

EJEMPLOS PARCIALES DE INSTRUMENTOS PARA LA GESTIÓN DE LA SEGURIDAD

La evaluación de riesgos implica el uso sistemático de información para identificar, analizar y evaluar los riesgos. Los ejemplos parciales de las figuras B.1, B.2, B.3 y B.4 ilustran instrumentos sencillos para emprender cada una de esas etapas del proceso de gestión del riesgo.

Cada organización debería identificar y utilizar los instrumentos más apropiados para su realidad, cultura y actividades. No hay una solución única. Para ejemplos adicionales, véase a norma ISO/IEC 31010.

Archivo de referencia del riesgo						
Nombre del servicio:				Fecha del análisis crítico de riesgo:		
				Compilado por:		Fecha:
Actividades de turismo de aventura involucradas:				Revisado por:		Fecha:
Ref.	Escenario	Lugar de ocurrencia	Peligro: qué puede suceder y cómo	Consecuencias de un evento	Conseque as	

Figura B.1 Ejemplo de tabla de referencia de riesgos

Nivel	Descripción	Ejemplo de la descripción
1	Insignificante	Sin lesiones, pérdidas financieras menore
2	Menor	Tratamiento c
3	Moderado	Tratamiento
4	Mayor	Heridas
5		

Figura B.2 - Ejemplo de medidas cualitativas del nivel de consecuencias

Nivel	Descripción	Ejemplo de la descripción
A	Casi seguro	Se espera que ocurra la mayoría de las veces
B	Probable	Es probable que ocurra la mayoría de
C	Posible	Puede ocurrir alguna
D	Improbable	Es poco prob
E		
NOT		

Figura B.3 Ejemplo de medidas cualitativas de probabilidad

Nivel	Consecuencias			
	Insignificante	Menor	Moderada	
A (Casi seguro)				
B (Probable)				
C (Posible)				
D (Improbable)				
E (Raro)				

Clave:
E: Riesgo extr
H: Riesgo
M: Ri

Figura B.4 Ejemplo de clasificación de probabilidad y consecuencia - Matriz de análisis cualitativo de riesgos - Nivel de riesgos

BIBLIOGRAFÍA

[1] ISO 9000:2005, Quality Management Systems. Fundamentals and Vocabulary.

[2] ISO 19011, Guidelines for Auditing Management Systems.

[3] ISO/TR 21102, Adventure Tourism. Leaders. Personnel Competence.

[4] ISO 21103, Adventure Tourism. Information for Participants.

[5] ISO 31000, Risk Management. Principles and Guidelines.

[6] ISO Guide 73:2009, Risk Management. Vocabulary.

[7] IEC 31010, Risk Management. Risk Assessment Techniques.

DOCUMENTO DE REFERENCIA

INTERNATIONAL STANDARDIZATION ORGANIZATION. *Adventure Tourism. Safety Management Systems. Requirements*. Ginebra, ISO, 25 p, 2014 (ISO 21101:2014 revisado y confirmado 2019).

Colombia

Apartadó
apartado@icontec.org

Armenia
armenia@icontec.org

Barranquilla
barranquilla@icontec.org

Barrancabermeja
barrancabermeja@icontec.org

Bogotá
bogota@icontec.org

Bucaramanga
bucaramanga@icontec.org

Cali
cali@icontec.org

Cartagena
cartagena@icontec.org

Cúcuta
cucuta@icontec.org

Manizales
manizales@icontec.org

Medellín
medellin@icontec.org

Montería
monteria@icontec.org

Ibagué
ibague@icontec.org

Neiva
neiva@icontec.org

Pereira
pereira@icontec.org

Pasto
pasto@icontec.org

Villavicencio
villavicencio@icontec.org

Resto del mundo

Bolivia
bolivia@icontec.org

Ecuador
ecuador@icontec.org

Honduras
honduras@icontec.org

Panamá
panama@icontec.org

Costa Rica
costarica@icontec.org

El Salvador
elsalvador@icontec.org

México
mexico@icontec.org

República Dominicana
republicadominicana@icontec.org

Chile
chile@icontec.org

Guatemala
guatemala@icontec.org

Nicaragua
nicaragua@icontec.org

Perú
peru@icontec.org

Canales de atención al cliente:
Bogotá: **607 8888**
Resto del país: **01 8000 94 9000**
cliente@icontec.org
www.icontec.org

icontec.org