Sustento del uso justo de Materiales Protegidos

derechos de autor para fines educativos

UCI
Universidad para la Cooperación Internacional

UCI
Sustento del uso justo de materiales protegidos por
derechos de autor para fines educativos

El siguiente material ha sido reproducido, con fines estrictamente didácticos e ilustrativos de los temas en cuestión, se utilizan en el campus virtual de la Universidad para la Cooperación Internacional – UCI – para ser usados exclusivamente para la función docente y el estudio privado de los estudiantes pertenecientes a los programas académicos.

La UCI desea dejar constancia de su estricto respeto a las legislaciones relacionadas con la propiedad intelectual. Todo material digital disponible para un curso y sus estudiantes tiene fines educativos y de investigación. No media en el uso de estos materiales fines de lucro, se entiende como casos especiales para fines educativos a distancia y en lugares donde no atenta contra la normal explotación de la obra y no afecta los intereses legítimos de ningún actor.

La UCI hace un USO JUSTO del material, sustentado en las excepciones a las leyes de derechos de autor establecidas en las siguientes normativas:

a- Legislación costarricense: Ley sobre Derechos de Autor y Derechos Conexos, No.6683 de 14 de octubre de 1982 - artículo 73, la Ley sobre Procedimientos de Observancia de los Derechos de Propiedad Intelectual, No. 8039 – artículo 58, permiten el copiado parcial de obras para la ilustración educativa.
b- Legislación Mexicana; Ley Federal de Derechos de Autor; artículo 147.
c- Legislación de Estados Unidos de América: En referencia al uso justo, menciona: "está consagrado en el artículo 106 de la ley de derecho de autor de los Estados Unidos (U.S,Copyright - Act) y establece un uso libre y gratuito de las obras para fines de crítica, comentarios y noticias, reportajes y docencia (lo que incluye la realización de copias para su uso en clase)."
d- Legislación Canadiense: Ley de derechos de autor C-11– Referidos a Excepciones para Educación a Distancia.
e- OMPI: En el marco de la legislación internacional, según la Organización Mundial de Propiedad Intelectual lo previsto por los tratados internacionales sobre esta materia. El artículo 10(2) del Convenio de Berna, permite a los países miembros establecer limitaciones o excepciones respecto a la posibilidad de utilizar lícitamente las obras literarias o artísticas a título de ilustración de la enseñanza, por medio de publicaciones, emisiones de radio o grabaciones sonoras o visuales.

Además y por indicación de la UCI, los estudiantes del campus virtual tienen el deber de cumplir con lo que establezca la legislación correspondiente en materia de derechos de autor, en su país de residencia.

Finalmente, reiteramos que en UCI no lucramos con las obras de terceros, somos estrictos con respecto al plagio, y no restringimos de ninguna manera el que nuestros estudiantes, académicos e investigadores accedan comercialmente o adquieran los documentos disponibles en el mercado editorial, sea directamente los documentos, o por medio de bases de datos científicas, pagando ellos mismos los costos asociados a dichos accesos.

ISO 22301 FOUNDATION (I22301F)

CertiProf®

Professional Knowledge

www.certiprof.com

(I22301F) VERSIÓN 092020

Objetivos

- Alcance, propósito, términos y definiciones claves de la norma ISO 22301 y cómo puede ser utilizada.

¿Quién es CertiProf®?

CertiProf® es un instituto examinador fundado en Estados Unidos en 2015.Ubicado en Sunrise, Florida.

Nuestra filosofía se basa en la creación de conocimiento en comunidad y para ello su red colaborativa está conformada por:

- **CKA's (CertiProf Knowledge Ambassadors),** son personas influyentes en sus campos de experiencia o maestría, entrenadores, formadores, consultores, blogueros, constructores de comunidades, organizadores y evangelistas, que están dispuestos a contribuir en la mejora del contenido.
- **CLL's (CertiProf Lifelong Learners),** se identifican como aprendices continuos que han demostrado su compromiso inquebrantable con el aprendizaje permanente, que es de vital importancia en el mundo digitalizado en constante cambio y expansión de hoy. Independientemente de si ganan o no el examen.
- **ATP's (Accredited Trainer Partners)**. Universidades, centros de formación y facilitadores de todo el mundo que integran la red de socios.
- **Autores (co-creadores).** Expertos o practicantes de la industria que, con sus conocimientos, desarrollan contenidos para la creación de nuevas certificaciones que respondan a las necesidades de la industria.
- **Staff interno,** nuestro equipo distribuido con operaciones en India, Brasil, Colombia y Estados Unidos que apoyan día a día la ejecución del propósito de **CertiProf®.**

Our Accreditations and Affiliations

¿Quién debe atender este taller de certificación?

Cualquier persona que esté interesada en ampliar sus conocimientos en la **Norma ISO/IEC 22301.**

AGENDA

1. Introducción y Antecedentes

CertiProf®

Professional Knowledge

www.certiprof.com

Introducción

- ISO 22301.
- Beneficios de un SGCN.
- Historia de la Norma.
- Estado actual.

La norma especifica la estructura y los requisitos para la implantación y el mantenimiento de un Sistema de Gestión de Continuidad del Negocio (SGCN) que desarrolla la continuidad del negocio de manera apropiada a la magnitud y tipo de impacto que la organización puede o no aceptar luego de un incidente disruptivo.

Los resultados de mantener un SGCN están determinados por los requisitos legales, regulatorios, organizacionales e industriales, los productos o servicios ofrecidos, los procesos empleados, el tamaño, la estructura y los requisitos de las partes interesadas de la organización.

Un SGCN destaca la importancia de:

- Comprender las necesidades de la organización y la necesidad de establecer la política y los objetivos de la gestión de la continuidad del negocio.
- La operación y el mantenimiento de los procesos, las capacidades y las estructuras de respuesta para asegurar que la organización sobrevivirá a los incidentes disruptivos.
- Realizar el seguimiento y la revisión del desempeño y la eficacia del SGCN, y la mejora continua basada en mediciones cualitativas y cuantitativas.

Beneficios de SGCN

El propósito de un SGCN es preparar para, proveer y mantener controles y las capacidades para gestionar la habilidad global de una organización para continuar operando durante los incidentes disruptivos.

a) Desde una perspectiva de negocio:
   - Apoyando a sus objetivos estratégicos.
   - Creando una ventaja competitiva.
   - Protegiendo y fortaleciendo su reputación y credibilidad.
   - Contribuyendo a la resiliencia de la organización.

b) Desde una perspectiva financiera:
   - Reduciendo la exposición legal y financiera.
   - Reduciendo los costos directos e indirectos de los incidentes disruptivos.

c) Desde la perspectiva de las partes interesadas:
- Protegiendo la vida, la propiedad y el medioambiente.
- Considerando las expectativas de las partes interesadas.
- Proporcionando confianza en la capacidad de la organización de ser exitosa.

d) Desde la perspectiva de los procesos internos:
- Mejorando su capacidad de mantenerse eficaces durante los incidentes disruptivos.
- Demostrando proactividad en el control de los riesgos de forma eficaz y eficiente.
- Abordando las vulnerabilidades operacionales.

Historia de la Norma

Principales Cambios Realizados en la Norma ISO 22301

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

- Se han aplicado los requisitos de ISO para estándares de sistemas de gestión, que han evolucionado desde 2012.
- Los requisitos se han clarificado, no se han agregado requisitos nuevos.
- Los requisitos específicos de la disciplina de continuidad del negocio están ahora casi por completo dentro del capítulo 8.
- El requisito 8 se ha reestructurado para proporcionar una comprensión más clara de los requisitos clave.
- Se han modificado varios términos específicos de la disciplina de continuidad del negocio para mejorar la claridad y reflejar el pensamiento actual.

2. Términos y Definiciones (Ver Anexo)

CertiProf®

Professional Knowledge

www.certiprof.com

3. Estructura de la Norma

CertiProf®

Professional Knowledge

www.certiprof.com

Estructura de ISO 22301

Introducción.
1. Objeto.
2. Referencias normativas.
3. Términos y definiciones.
4. Contexto de la organización.
5. Liderazgo.
6. Planificación.
7. Apoyo.
8. Operación.
9. Evaluación del desempeño.
10. Mejora.

Bibliografía.

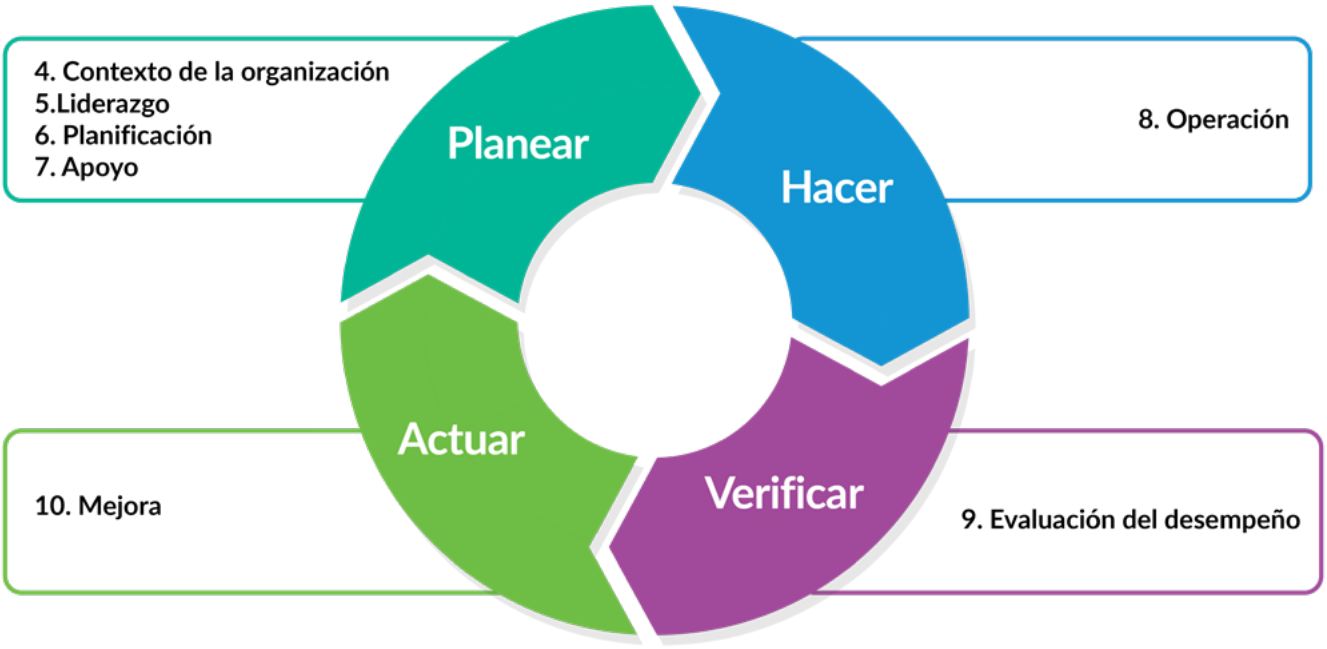
Introducción

La norma ISO 22301 cumple con los requisitos de las normas de sistemas de gestión de ISO. Estos requisitos incluyen una estructura de alto nivel, texto básico idéntico y términos comunes con definiciones centrales, diseñados para beneficiar a los usuarios que implementan múltiples normas del sistema de gestión ISO.

La norma ISO 22301 contiene requisitos que una organización puede utilizar para implementar un SGCN y evaluar la conformidad.

Estructura de la ISO 22301

Ciclo PHVA Y SGCN



Estructura de ISO 22301

- **1. Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos.**

Esta norma especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse contra, reducir la probabilidad de ocurrencia, prepararse para, responder a y recuperarse de incidentes disruptivos que puedan surgir.

Esta Norma Internacional es aplicable a todos los tipos y tamaños de organizaciones que:

a) Deseen implementar, mantener y mejorar un SGCN.
b) Busquen asegurar la conformidad con la política de continuidad de negocio establecida.
c) Necesiten poder continuar con la entrega de sus productos o servicios durante un incidente disruptivo con una capacidad aceptable predefinida.
d) Busquen fortalecer su resiliencia mediante la aplicación eficaz del SGCN.

Este documento puede ser utilizado para evaluar la capacidad de una organización para satisfacer sus necesidades y sus obligaciones de continuidad.

- **2. Referencias normativas.**

Proporciona detalles sobre las normas de referencia o publicaciones relevantes en relación a la norma concreta.
Como es la ISO 22300, Seguridad y resiliencia. Vocabulario

- **3. Términos y definiciones.**

Detalla términos y definiciones aplicables a la norma específica, además de cualquier otro término y definición relacionado con la norma.

- **4. Contexto de la organización.**
- **4.1 Comprensión de la organización y de su contexto.**
- **4.2 Compresión de las necesidades y expectativas de las partes interesadas.**
- **4.3 Determinación del alcance del SGCN.**
- **4.4 Sistema de gestión de la continuidad del negocio.**

4. Contexto de la Organización

CertiProf®

Professional Knowledge

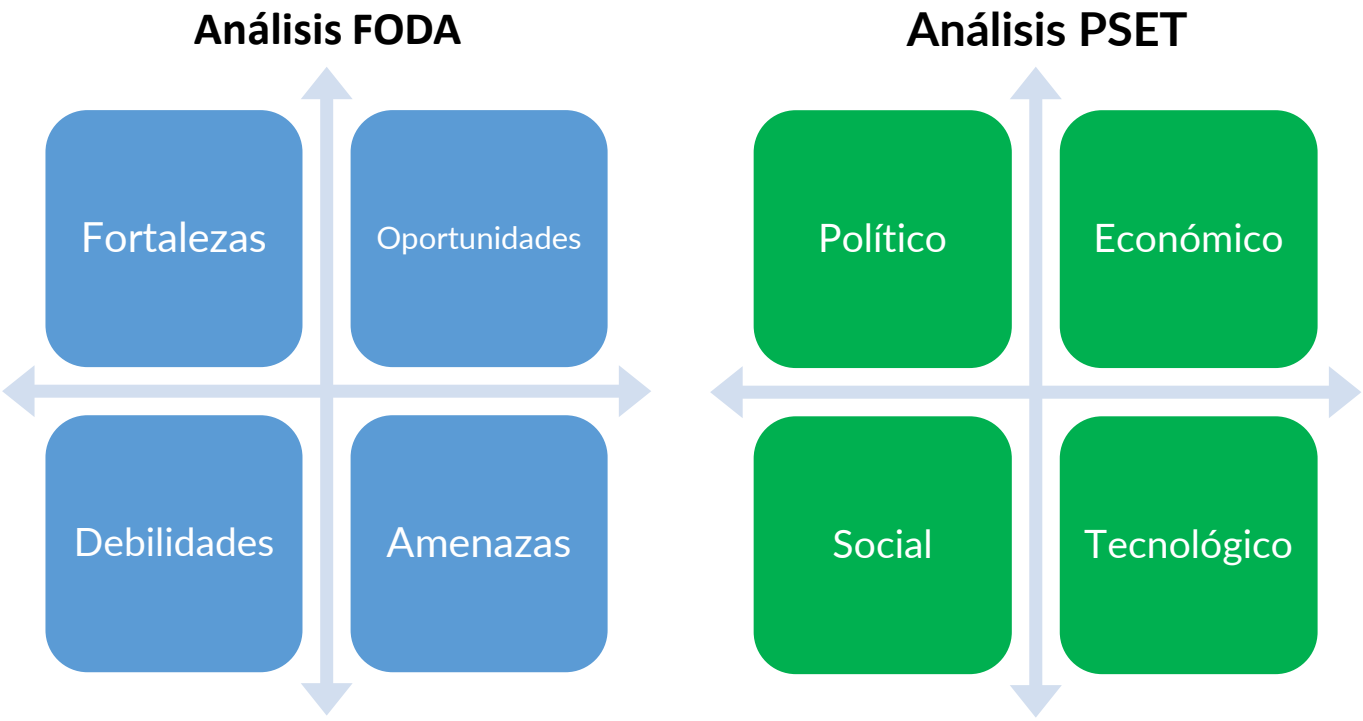
www.certiprof.com

4.1 Comprensión de la Organización y de su Contexto

La organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad de lograr los resultados deseados de su SGCN.

NOTA: Estas cuestiones pueden estar afectadas por los objetivos generales de la organización, sus productos y servicios y el tipo y nivel de riesgo que puede o no aceptar.

Para determinar el contexto podemos utilizar alguna de estas herramientas:



4.2 Compresión de las Necesidades y Expectativas de las Partes Interesadas

4.2.1 Generalidades

Al establecer su SGCN, la organización debe determinar:
a) Las partes interesadas que son pertinentes para el SGCN.
b) Los requisitos pertinentes de esas partes interesadas.

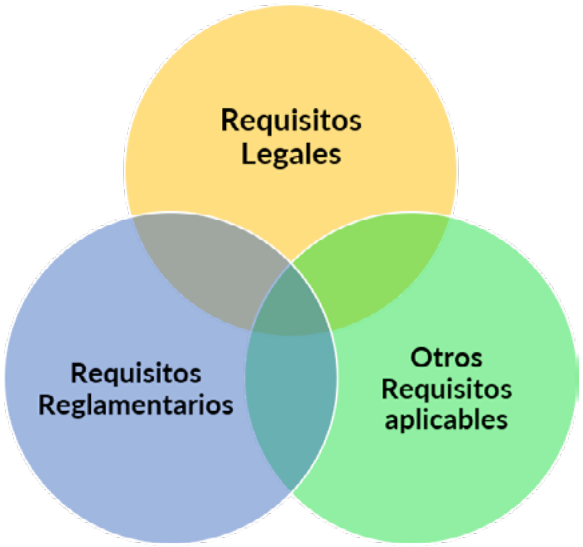
Ejemplo de partes interesadas:

- Accionistas.
- Gerencia.
- Personal Interno.
- Contratistas.
- Proveedores.
- Clientes.
- Entidades Reguladoras.
- Gobierno.
- Competidores.
- Grupos de Interés.

4.2.2 Los requisitos legales y reglamentarios

La organización debe:

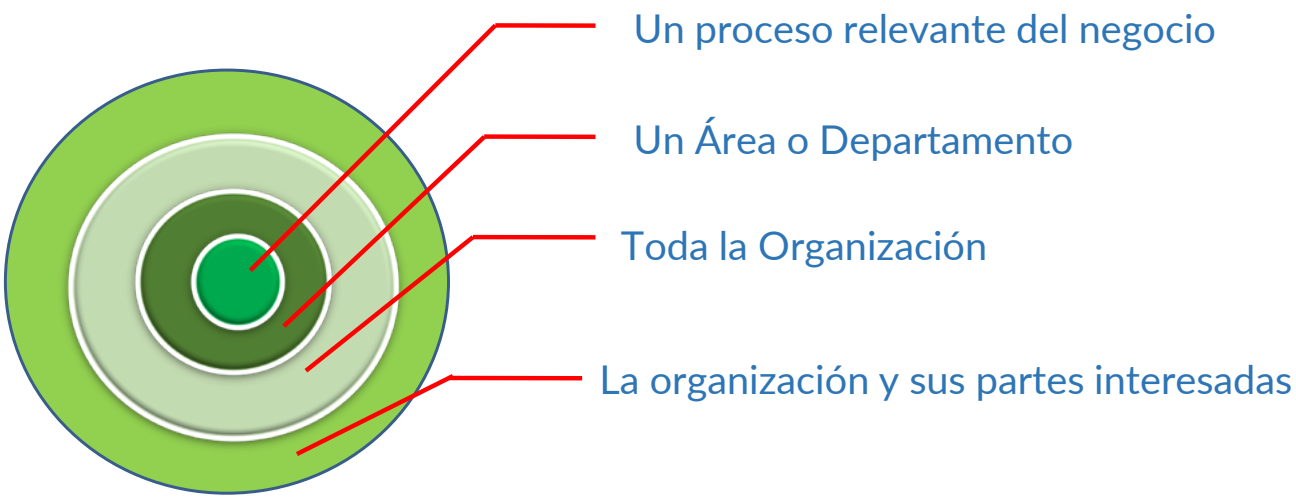
a) Implementar y mantener un proceso para identificar, tener acceso a y evaluar los requisitos legales y reglamentarios relacionados con la continuidad de sus productos, servicios, actividades y recursos.
b) Asegurarse de que estos requisitos legales, reglamentarios y otros aplicables se tengan en cuenta en la implementación y el mantenimiento de su SGCN.
c) Documentar esta información y mantenerla actualizada.



Taller Sobre Requisitos 4.1 y 4.2

4.3 Determinación del Alcance del SGCN

La organización debe determinar los límites y la aplicabilidad del SGCN para establecer su alcance.



4.3.1 Generalidades

La organización debe determinar los límites y la aplicabilidad del SGCN para establecer su alcance.

Al determinar el alcance, la organización debe considerar:
a) Las cuestiones internas y externas indicados en el apartado 4.1.
b) Los requisitos indicados en el apartado 4.2.
c) La misión, los objetivos y las obligaciones internas y externas.

El alcance debe estar disponible como información documentada.

4.3.2 Alcance del SGCN

La organización debe:
a) Establecer las partes de la organización a ser incluidas en el SGCN, teniendo en cuenta sus localizaciones, tamaño, naturaleza y complejidad.
b) Identificar los productos y servicios a ser incluidos en el SGCN.

Al definir el alcance, la organización debe documentar y explicar las exclusiones.

Las exclusiones deben ser explicadas. Las mismas no deben afectar la capacidad y la responsabilidad de la organización de proveer continuidad del negocio y de las operaciones que cumplan con los requisitos del SGCN, según lo determinado por el análisis de impacto en el negocio o la evaluación de riesgos y los requisitos legales o reglamentarios.

4.4 Sistema de Gestión de la Continuidad del Negocio

Sistema de Gestión de la Continuidad del Negocio

La organización debe establecer, implementar, mantener y mejorar continuamente un SGCN, incluyendo los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

5. Liderazgo

CertiProf®

Professional Knowledge

www.certiprof.com

Liderazgo

- 5. Liderazgo.
  - 5.1 Liderazgo y compromiso.
  - 5.2 Política.
  - 5.3 Roles, responsabilidades y autoridades.

5.1 Liderazgo y Compromiso

La alta dirección debe demostrar su liderazgo y compromiso con respecto al SGCN:

a) Asegurándose de que se establezcan la política y los objetivos para el SGCN, y que éstos son compatibles con la dirección estratégica de la organización.
b) Asegurándose de la integración de los requisitos del SGCN con los procesos de negocio de la organización.
c) Garantizar que los recursos necesarios para el SGCN estén disponibles.
d) Comunicar la importancia de una efectiva continuidad del negocio y la conforme con los requisitos del SGCN.
e) Garantizar que el SGCN logre los resultados previstos.
f) Dirigiendo y apoyando a las personas para contribuir a la eficacia del SGCN.
g) Promoviendo la mejora continua.
h) Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo y compromiso en la forma en la que aplique a sus áreas de responsabilidad.

NOTA: este documento puede ser interpretado en términos generales en el sentido de aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

5.2.1 Establecer la política de continuidad del negocio

La alta dirección debe establecer una política de continuidad del negocio que:

a) Sea apropiada al propósito de la organización.
b) Proporcione un marco de referencia para establecer los objetivos de continuidad del negocio.
c) Incluya un compromiso para satisfacer los requisitos aplicables.
d) Incluya un compromiso de mejora continua del SGCN.

5.2.2 Comunicación de la política

La política de continuidad del negocio debe:

a) Estar disponible como información documentada.
b) Ser comunicada dentro de la organización.
c) Estar disponible para las partes interesadas, según corresponda.

5.3 Roles, Responsabilidades y Autoridades

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

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurar que el SGCN cumpla con los requisitos de este documento.
b) Informar sobre el desempeño del SGCN a la alta dirección.

6. Planificación

CertiProf®

Professional Knowledge

www.certiprof.com

Planificación

- 6. Planificación.
  - 6.1 Acciones para tratar riesgos y oportunidades.
  - 6.2 Objetivos de la continuidad del negocio y planificación para lograrlos.
  - 6.3 Planificación de los cambios del SGCN.

6.1 Acciones para Abordar Riesgos y Oportunidades

6.1.1 Determinación de riesgos y oportunidades

Al planificar el SGCN, la organización debe considerar las cuestiones referidas en el apartado 4.1 y los requisitos referidos en el apartado 4.2, y determinar los riesgos y oportunidades que es necesario abordar con el fin de:

a) Asegurar que el SGCN puede lograr los resultados deseados.
b) Prevenir o reducir efectos no deseados.
c) Lograr la mejora continua.

6.1.2 Abordar riesgos y oportunidades

La organización debe planificar:

a) Las acciones para abordar estos riesgos y oportunidades.
b) Cómo integrar e implementar las acciones en sus procesos del SGCN (Véase 8.1).
c) Evaluar la eficacia de estas acciones (Véase 9.1).

NOTA: Los riesgos y oportunidades se relacionan con la eficacia del sistema de gestión. Los riesgos relacionados con los incidentes disruptivos del negocio son abordados en 8.2.

6.2 Objetivos de la Continuidad del Negocio y Planificación para Lograrlos

6.2.1 Establecimiento de los objetivos de continuidad del negocio

La organización debe establecer los objetivos de la continuidad del negocio para las funciones y niveles pertinentes.

Los objetivos de la continuidad del negocio deben:

a) Ser coherentes con la política de continuidad del negocio.
b) Ser medibles (si es posible).
c) Tener en cuenta los requisitos aplicables (véase 4.1 y 4.2).
d) Ser objeto de seguimiento.
e) Comunicarse.
f) Actualizarse, según corresponda.

La organización debe mantener información documentada sobre los objetivos de continuidad del negocio.

6.2.2 Determinación de los objetivos de continuidad del negocio

Al planificar cómo lograr sus objetivos de continuidad del negocio, la organización debe determinar:

a) Qué se va a hacer.
b) Qué recursos se requerirán.
c) Quién será responsable.
d) Cuándo se finalizará.
e) Cómo se evaluarán los resultados.

6.3 Planificación de los Cambios del SGCN

Cuando la organización determine la necesidad de cambios en el SGCN , incluyendo los identificados en el Capítulo 10, estos cambios se deben llevar a cabo de manera planificada.

La organización debe considerar:

a) El propósito de los cambios y sus consecuencias potenciales.
b) La integridad del SGCN.
c) La disponibilidad de recursos.
d) La asignación o reasignación de responsabilidades y autoridades.

7. Apoyo (Soporte)

CertiProf®

Professional Knowledge

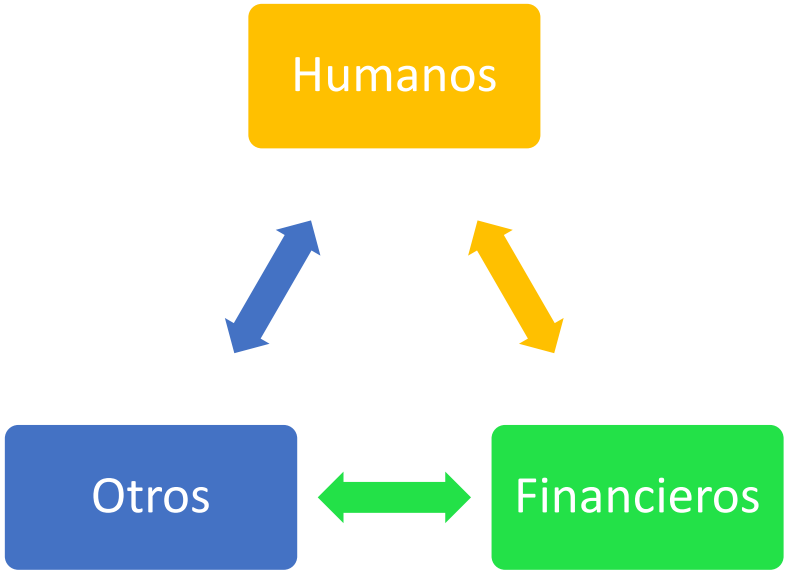
www.certiprof.com

Apoyo

- 7. Apoyo.
  - 7.1 Recursos.
  - 7.2 Competencia.
  - 7.3 Conciencia.
  - 7.4 Comunicación.
  - 7.5 Información documentada.

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, la implementación, el mantenimiento y la mejora continua del SGCN.



7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta al desempeño de la continuidad del negocio.

b) Asegurarse de que éstas personas sean competentes, basándose en la educación, formación o experiencia apropiadas.

c) cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas.

d) conservar la información documentada apropiada como evidencia de la competencia.

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

7.3 Concienciación

Las personas que realizan trabajos bajo el control de la organización deben tomar conciencia de:

a) La política de continuidad del negocio.
b) Su contribución a la eficacia del SGCN, incluyendo los beneficios de una mejora en el desempeño de la gestión de continuidad del negocio.
c) Las implicaciones del incumplimiento de los requisitos del SGCN.
d) Su propio rol y responsabilidades antes, durante y después de los incidentes disruptivos.

7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGCN que incluyan:

a) Qué comunicar.
b) Cuándo comunicar.
c) A quién comunicar.
d) Cómo comunicar.
e) Quién comunica.

7.5 Información Documentada

7.5.1 Generalidades

El SGCN de la organización debe incluir:

a) La información documentada requerida por este documento.
b) La información documentada que la organización determine como necesaria para la eficacia del SGCN.

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

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

7.5.2 Elaboración y actualización

Al elaborar y actualizar la información documentada, la organización debe asegurarse de que lo siguiente sea apropiado:

a) Identificación y descripción (por ejemplo, título, fecha, autor o número de referencia).
b) Formato (el idioma, versión de software, gráficos), y los medios de soporte (por ejemplo, papel, electrónico).
c) La revisión y aprobación con respecto a la conveniencia y adecuación.

7.5.3 Control de la información documentada

7.5.3.1 La información documentada requerida por el SGCN y por este documento se debe controlar para asegurar de que:

a) Esté disponible y sea idónea para su uso, donde y cuando se necesite.
b) Esté protegida adecuadamente (por ejemplo, contra pérdida de la confidencialidad, uso inadecuado o pérdida de la integridad).

7.5.3.2 Para el control de la información documentada la organización debe abordar las siguientes actividades, según corresponda:

a) Distribución, acceso, recuperación y uso.
b) Almacenamiento y preservación, incluida la preservación de la legibilidad.
c) Control de cambios (por ejemplo, control de versión).
d) Retención y disposición.
e) La información documentada de origen externo, que la organización determina como necesaria para la planificación y la operación del SGCN, se debe identificar, según sea apropiado, y controlar.

NOTA: el acceso puede implicar una decisión en relación al permiso, solamente para consultar la información documentada, o al permiso y a la autoridad para consultar y modificar la información documentada.

8. Operación

CertiProf®

Professional Knowledge

www.certiprof.com

Operación

- 8. Operación.
  - 8.1 Planificación operacional y control.
  - 8.2 Análisis de impacto en el negocio y evaluación de riesgos.
  - 8.3 Estrategias de continuidad del negocio y soluciones.
  - 8.4 Planes y procedimientos de continuidad del negocio.
  - 8.5 Programa de ejercicios.
  - 8.6 Evaluación de la documentación y capacidades de continuidad del negocio.

8.1 Planificación Operacional y Control

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en el apartado 6.1 mediante:

a) La determinación de los criterios para los procesos.
b) La implementación del control de los procesos de acuerdo con los criterios.
c) La conservación de la información documentada en la extensión necesaria para tener confianza en que los procesos se han llevado a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no deseados, tomando acciones para mitigar cualquier efecto adverso, según sea necesario.

La organización debe asegurarse de que los procesos subcontratados son controlados.

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.1 Generalidades

La organización debe:

a) Implementar, y mantener un proceso sistemático para el análisis de impacto en el negocio y la evaluación de riesgos de incidentes disruptivos.
b) Revisar el análisis de impacto del negocio y la evaluación de riesgos a intervalos planificados y cuando existan cambios significativos, en la organización o su contexto en el que opera.

NOTA: la organización determina como se realiza el análisis de impacto en el negocio y la evaluación de riesgos.

8.2.2 Análisis del impacto en el negocio

La organización debe usar el proceso de análisis de impacto del negocio para determinar las prioridades y los requisitos de continuidad del negocio. El proceso debe:

a) Definir los tipos de impacto y los criterios pertinentes para el contexto de la organización.
b) La identificación de actividades que soportan el suministro de productos y servicios.
c) Usar los tipos de impactos y los criterios para evaluar los impactos con el transcurso del tiempo resultantes de la interrupción de estas actividades.
d) Identificar los plazos de tiempo en los cuales los impactos de no reanudar la actividades serían inaceptables para la organización.

NOTA 1: esto puede referirse como el **período máximo tolerable de interrupción MTPD** (por sus siglas en inglés, **maximum tolerable period of disruption).**

e) establecer períodos de tiempo prioritarios en el tiempo identificado en d) para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada.

NOTA 2: este período de tiempo puede ser denominado como **objetivo de tiempo de recuperación RTO** (por sus siglas en inglés, **Recovery Time Objective)**.

f) Utilizar el análisis para identificar las actividades prioritarias.
g) Determinar los recursos que son necesarios para soportar las actividades prioritarias.
h) Determinar las dependencias, incluyendo socios y proveedores, y las interdependencias de las actividades prioritarias.

Taller 2: Análisis de Impacto en el Negocio (BIA)

8.2 Análisis de Impacto en el Negocio y Evaluación de Riesgos

8.2.3 Evaluación de riesgos

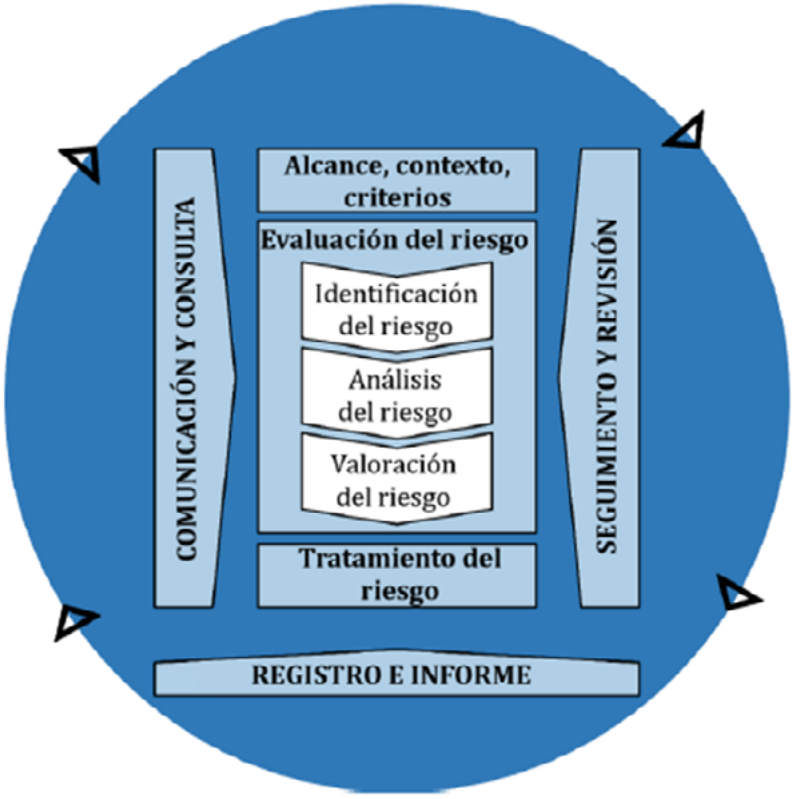
La organización debe implementar y mantener un proceso de evaluación de riesgos.

NOTA: En la norma ISO 31000 se aborda el proceso para la evaluación de riesgos.

La organización debe:
a) Identificar los riesgos de incidentes disruptivos para las actividades prioritarias de la organización y de sus recursos.
b) Analizar y valorar los riesgos identificados.
c) Determinar cuáles riesgos requieren tratamiento.

NOTA: los riesgos en este apartado son los relacionados con los incidentes disruptivos de las actividades del negocio. Los riesgos y oportunidades relacionados con la eficacia del sistema de gestión se abordan en 6.1.

PROCESO DE GESTION DE RIESGOS SEGÚN ISO 31000



8.3 Estrategias de Continuidad del Negocio y Soluciones

8.3.1 Generalidades

Basándose en las salidas del análisis de impacto del negocio y la evaluación de riesgos, la organización debe identificar y seleccionar las estrategias de continuidad del negocio que considere las opciones para antes, durante y después de un incidente disruptivo.

Las estrategias de continuidad del negocio deben comprender una o más soluciones.

8.3.2 Identificación de estrategias y soluciones

La identificación debe basarse en estrategias y soluciones que:

a) Cumplan con los requisitos de continuidad y recuperación de las actividades prioritarias en el marco de tiempo identificado y la capacidad acordada.
b) Protejan las actividades prioritarias de la organización.
c) Reduzcan la probabilidad de un incidente disruptivo.
d) Acorten los períodos de interrupción.
e) Limiten los impactos de los incidentes disruptivos en los productos y servicios de la organización.
f) Provean de la disponibilidad de los recursos adecuados.

8.3.3 Selección de las estrategias y soluciones

La selección debe basarse en estrategias y soluciones que:

a) Cumplan con los requisitos de continuidad y recuperación de las actividades prioritarias en el marco de tiempo identificado y la capacidad acordada.
b) Consideren el tipo y nivel de riesgo que la organización puede o no aceptar.
c) Considere los costos y beneficios asociados.

8.3.4 Requisitos de recursos

La organización debe determinar los requisitos de recursos para implementar las soluciones de continuidad de negocio seleccionadas. Los tipos de recursos considerados deben incluir, pero no limitarse a:

a) Las personas.
b) La información y los datos.
c) Infraestructura física como los edificios, el ambiente de trabajo y otras infraestructuras y servicios asociados.
d) Los equipos y los insumos.
e) Los sistemas de tecnología de la información y la comunicación (TIC).
f) El transporte y la logística.
g) Las finanzas.
h) Los socios y proveedores.

8.3.5 Implementación de la solución

La organización debe implementar y mantener las soluciones seleccionadas de continuidad del negocio para que puedan ser activadas cuando sea necesario.

8.4 Planes y Procedimientos de Continuidad del Negocio

8.4.1 Generalidades

La organización debe implementar y mantener una estructura de respuesta que permitirá la advertencia y comunicación oportuna a las partes interesadas pertinentes. La organización debe proveer de los planes y procedimientos para gestionar la organización durante el incidente disruptivo.

Los planes y procedimientos deben ser utilizados cuando sea necesario activar las soluciones de continuidad del negocio.

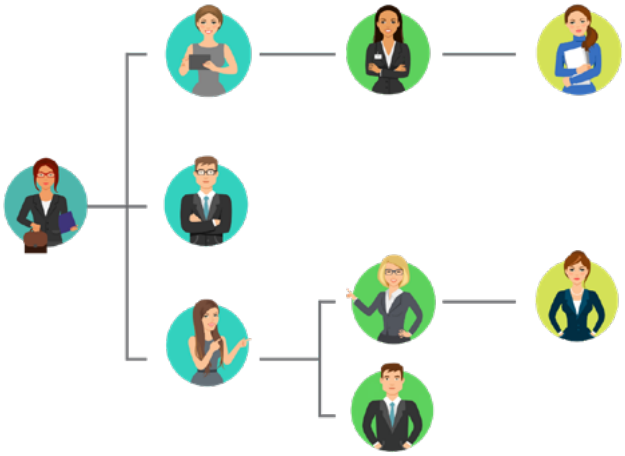
NOTA: existen distintos tipos de procedimientos que constituyen los planes de continuidad de negocio.

La organización debe identificar y documentar los planes y procedimientos de continuidad del negocio basándose en las salidas de las estrategias y soluciones seleccionadas.
Los procedimientos deben:

a) Ser específicos con respecto a las etapas inmediatas que deben tomarse durante un incidente disruptivo.
b) Ser flexibles para responder a los cambios en las condiciones internas y externas de un incidente disruptivo.
c) Enfocarse en el impacto de los incidentes que potencialmente podrían ser incidentes disruptivos.
d) Ser eficaces minimizando el impacto a través de la implementación de las soluciones apropiadas.
e) Asignar los roles y las responsabilidades para las tares durante los mismos.

8.4.2 Estructura de respuesta

8.4.2.1 La organización debe implementar y mantener una estructura, identificando uno o más equipos responsables de dar respuesta a un incidente disruptivo.



8.4.2.2 Los roles y responsabilidades de cada equipo y las relaciones entre los equipos deben ser establecidos claramente.

8.4.2.3 En forma colectiva, los equipos deben ser competentes para:

a) Evaluar la naturaleza y el alcance de un incidente disruptivo y su impacto potencial.
b) Evaluar el impacto con límites predefinidos que justifican el inicio de una respuesta formal.
c) Activar una respuesta apropiada de continuidad del negocio.
d) Planificar las acciones que necesitan ser realizadas.
e) Establecer prioridades (utilizando la seguridad de la vida como primera prioridad).
f) Realizar seguimiento a los efectos del incidente disruptivo y la respuesta de la organización.
g) Activar las soluciones de continuidad del negocio.
h) Comunicarse con las partes interesadas pertinentes, las autoridades y los medios.

8.4.2.4 Para cada equipo debe existir:

a) Personal identificado y sus suplentes con la responsabilidad necesaria, la autoridad y competencia para cumplir con el rol designado.
b) Procedimientos documentados para guiar sus acciones (ver 8.4.4), incluyendo aquellas para la activación, operación, coordinación y comunicación de la respuesta.

8.4.3 Alertas y comunicación

La organización debe documentar y mantener procedimientos para:

a) la comunicación interna y externa con las partes interesadas pertinentes, incluyendo qué, cuando, a quién y cómo comunicar.

NOTA: la organización puede documentar y mantener procedimientos sobre cómo y bajo qué circunstancias la organización comunica a sus empleados y los contactos de emergencia.

b) Recibir, documentar y responder a las comunicaciones de las partes interesadas, incluyendo cualquier sistema de alerta de riesgo nacional o regional o equivalente.
c) Asegurar la disponibilidad de los medios de comunicación durante un incidente disruptivo.
d) Facilitar la comunicación estructurada con los servicios de respuesta de emergencia.
e) Suministrar detalles sobre la repuesta de la organización a los medios siguiendo un incidente, incluyendo una estrategia de comunicación.
f) Registrar los detalles sobre el incidente disruptivo, las acciones llevadas a cabo, y las decisiones tomadas.

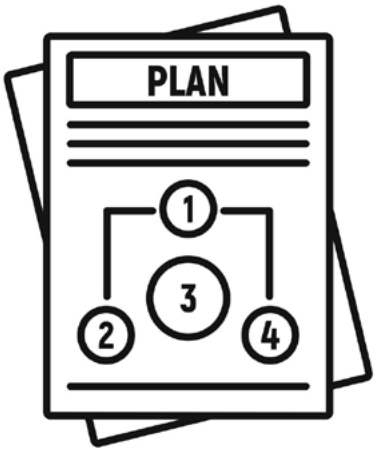
8.4.3.2 Cuando sea aplicable, también debe considerarse e implementarse lo siguiente:

a) Alertar a las partes interesadas potencialmente afectadas por un incidente disruptivo real o inminente.
b) Asegurar la adecuada coordinación y comunicación entre las múltiples organizaciones de respuesta.

Los procedimientos de alerta y comunicación deben ser ejercitados como parte del programa de ejercicios indicado en 8.5.

8.4.4 Planes de continuidad del negocio

8.4.4.1 la organización debe documentar y mantener planes y procedimientos de continuidad del negocio. Los planes de continuidad del negocio deben bridar orientación e información para apoyar a los equipos en la respuesta a un incidente disruptivo y dar apoyo a la organización con la respuesta y la recuperación.



8.4.4.2 En su conjunto los planes de continuidad del negocio deben contener:

a) Los detalles de las acciones que los equipos realizaran para:
   1. Continuar y recuperar las actividades prioritarias en un período de tiempo predeterminado.
   2. Realizar el seguimiento del impacto del incidente disruptivo y la respuesta de la organización al mismo.
b) Una referencia a los límites predefinidos y los procesos para activar la respuesta.
c) Los procedimientos que permitan suministrar los productos y servicios a una capacidad acordada.
d) Los detalles para gestionar inmediatamente las consecuencias de un incidente disruptivo teniendo en cuenta:
   1. El bienestar de los individuos.
   2. La prevención de pérdidas mayores o la inviabilidad de actividades prioritarias.
   3. El impacto en el medioambiente.

8.4.4.3 Cada plan debe incluir:

a) El propósito, alcance y objetivos.
b) Los roles y responsabilidades del equipo que implementará el plan.
c) Las acciones para implementar las soluciones.
d) La información de apoyo necesaria para activar (incluyendo los criterios de activación), operar, coordinar y comunicar las acciones del equipo.
e) Las interdependencias internas y externas.
f) Los recursos necesarios.
g) Los requisitos de informes.
h) Un proceso para retirarse del mercado.

Cada plan debe ser usado y estar disponible en el momento y lugar en que sea necesario.

8.4.5 Recuperación

La organización debe tener procesos documentados para restaurar y volver a las actividades de negocios de las medidas temporales adoptadas durante y después de un incidente.

8.5 Programa de Ejercicios

La organización debe implementar y mantener un programa de ejercicios y prueba para validar en el tiempo la eficacia de sus estrategias y soluciones de continuidad del negocio. La organización debe llevar a cabo ejercicios y pruebas que:

a) Sean coherentes con los objetivos de continuidad del negocio.
b) Se basen en escenarios apropiados que están bien planificados con metas y objetivos claramente definidos.
c) Desarrollen equipo de trabajo, competencias, confianza y conocimiento para aquellos que tienen roles que desempeñar relacionados con los incidentes disruptivos.
d) Tomados en conjunto, a través del tiempo validen sus estrategias y soluciones de continuidad del negocio.
e) Realicen informes formales post-ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras.
f) Sean revisados en el contexto de promover la mejora continua.
g) Sean llevados a cabo a intervalos planificados y cuando hayan cambios significativos dentro de la organización o en el contexto en el que opera.

La organización debe actuar sobre los resultados de sus ejercicios y pruebas para implementar los cambios y mejoras.

8.6 Evaluación de la Documentación y Capacidades de Continuidad del Negocio

La organización debe:

a) Evaluar la adecuación y eficacia del análisis de impacto del negocio, la evaluación de riesgo, las estrategias, soluciones, los planes y procedimientos.
b) Llevar a cabo evaluaciones mediante revisiones, análisis, ejercicios, pruebas, informes posteriores a un incidente y evaluaciones de desempeño.
c) Realizar evaluaciones de la capacidad de continuidad del negocio de los socios y partes interesadas pertinentes.
d) Evaluar el cumplimiento con los requisitos legales y reglamentarios aplicables, las buenas prácticas industriales y la conformidad con sus propios políticas y objetivos de continuidad del negocio.
e) Actualizar la documentación y los procedimientos de forma oportuna.

Estas evaluaciones deben ser realizadas a intervalos planificados, después de un incidente o activación, y cuando ocurran cambios significativos.

9. Evaluación y Desempeño

CertiProf®

Professional Knowledge

www.certiprof.com

Evaluación del Desempeño

- 9. Evaluación del desempeño.
  - 9.1 Seguimiento, medición, análisis y evaluación.
  - 9.2 Auditoria interna.
  - 9.3 Revisión por la dirección.

9.1 Seguimiento, Medición, Análisis y Evaluación

9.1.1 Generalidades

La organización debe determinar:

a) Qué necesita seguimiento y medición.
b) Los métodos de seguimiento, medición, análisis y evaluación necesarios para asegurar resultados válidos.
c) Cuándo y quiénes deben llevar a cabo el seguimiento y la medición.
d) Cuándo y quiénes se deben analizar y evaluar los resultados del seguimiento y la medición.

La organización debe conservar la información documentada apropiada como evidencia de los resultados.

La organización debe evaluar el desempeño y la eficacia del SGCN.

9.2 Auditoría Interna

9.2.1 Generalidades

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre como el SGCN.

a) Es conforme con:
   1. Los requisitos propios de la organización para su SGCN.
   2. Los requisitos de este documento.
b) Es eficazmente implementado y mantenido.

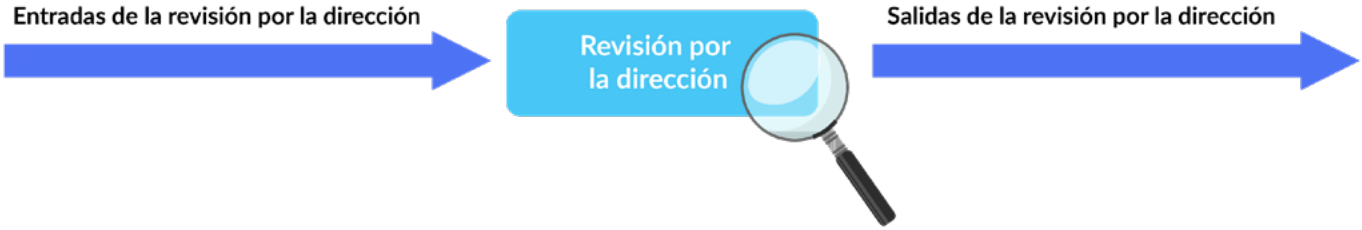
9.2.2 Programas de auditorías

La organización debe:

a) Planificar, establecer, implementar y mantener uno o varios programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que deben tener en consideración la importancia de los procesos involucrados, los cambios que afecten a la organización y los resultados de las auditorías previas.
b) Definir los criterios de la auditoría y el alcance para cada auditoría.
c) Seleccionar los auditores y llevar a cabo auditorías para asegurarse de la objetividad y la imparcialidad del proceso de auditoría.
d) Asegurarse de que los resultados de las auditorías se informen a los gerentes pertinentes.
e) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías.
f) Asegurarse que se toman las acciones correctivas necesaria sin demora injustificada para eliminar las no conformidades y sus causas.
g) Asegurarse que las acciones de seguimiento de las auditorías incluyen la verificación de las acciones tomadas y el informe de los resultados de las verificaciones.

9.3 Revisión por la Dirección

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



9.3.2 Entradas de la revisión por la dirección

La revisión por la dirección debe incluir consideraciones sobre:

a) El estado de las acciones de las revisiones por la dirección previas.
b) Los cambios en las cuestiones externas e internas que sean pertinentes al SGCN.
c) La información sobre el desempeño del SGCN, incluidas las tendencias relativas a:
    1. Las no conformidades y acciones correctivas.
    2. Los resultados de seguimiento y medición.
    3. Los resultados de las auditorías.
d) La retroalimentación de las partes interesadas.
e) La necesidad de cambios en el SGCN, incluyendo la política y los objetivos.
f) Los procedimientos y recursos que pueden ser usados por la organización para mejorar el desempeño y la eficacia del SGCN.
g) Información sobre el análisis de impacto del negocio y la evaluación de riesgos.
h) Las salidas de la evaluación de la documentación y capacidades relacionadas con la continuidad del negocio.
i) Los riesgos o cuestiones que no han sido abordados adecuadamente en una evaluación previa de riesgos.
j) Las lecciones aprendidas y las acciones que surgieron de los incidentes o incidentes disruptivos.
k) Las oportunidades de mejora continua.

9.3.3 Resultados de la revisión por la dirección

9.3.3.1 las salidas de la revisión por la dirección deben incluir las decisiones y acciones relacionadas con las oportunidades de mejora; cualquier necesidad de cambio en el SGCN y las necesidades de cambio del SGCN para mejorar la eficacia y eficiencia, incluyendo lo siguiente:

a) Variaciones en el alcance del SGCN.
b) La actualización del análisis de impacto del negocio, de la evaluación de riesgos, , de las estrategias de continuidad de negocios, y las soluciones y los planes de continuidad del negocio.
c) La modificación de los procedimientos y controles para responder a las cuestiones internas o externos que puedan impactar en el SGCN.
d) Cómo se medirá la eficacia de los controles.

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

La organización debe:

a) Comunicar los resultados de la revisión de gestión a las partes interesadas pertinentes.
b) Tomar las acciones apropiadas relacionadas con esos resultados.

10. Mejora

CertiProf®

Professional Knowledge

www.certiprof.com

Mejora

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

10.1 No Conformidad y Acción Correctiva

10.1.1 La organización debe determinar las oportunidades para mejora e implementar cualquier acción necesaria para lograr los resultados deseados de su SGCN.

10.1.2 Cuando ocurra una no conformidad, la organización debe:

a) Reaccionar ante la no conformidad y, cuando sea aplicable:
   1. Tomar acciones para controlarla y corregirla.
   2. Hacer frente a las consecuencias.

b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante:
   1. La revisión de la no conformidad.
   2. La determinación de las causas de la no conformidad.
   3. La determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir.

c) Implementar cualquier acción necesaria.
d) Revisar la eficacia de cualquier acción correctiva tomada.
e) Si fuera necesario, hacer cambios al SGCN.

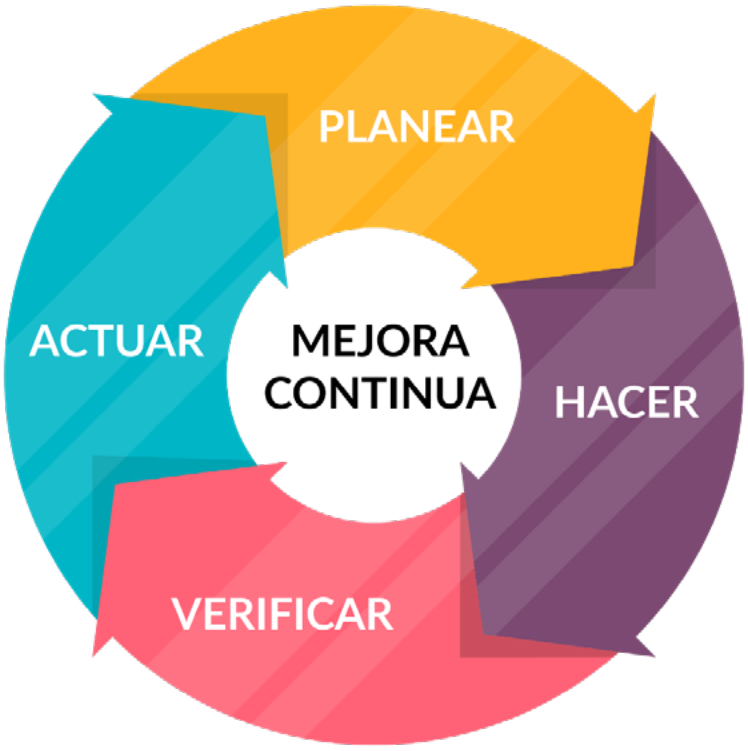
Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

10.1.3 La organización debe conservar la información documentada como evidencia de:

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

10.2 Mejora Continua

La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGCN basado en mediciones cualitativas y cuantitativas.



La organización debe mejorar continuamente la conveniencia, adecuación y eficacia del SGCN basado en mediciones cualitativas y cuantitativas.

La organización debe considerar los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades relacionadas con la continuidad del negocio o con el SGCN, que deben considerarse como parte de la mejora continua.

NOTA: la organización puede usar los procesos del SGCN como el liderazgo, la planificación, y la evaluación de desempeño para lograr la mejora.

Anexo 1: Términos y Definiciones

CertiProf®

Professional Knowledge

www.certiprof.com

3.1 Actividad

Conjunto de una o más tareas con una salida definida.

[Fuente: ISO 22300:2018, 3.1 modificado. La definición ha sido reemplazada y se eliminó el ejemplo]

3.2 Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- **NOTA 1:** Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
- **NOTA 2:** La auditoría interna la realiza la propia organización (3.1.14) o una parte externa en su nombre.
- **NOTA 3:** "Evidencia de la auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.
- **NOTA 4:** los elementos fundamentales de una auditoría incluyen la determinación de la conformidad de un objeto de acuerdo a un procedimiento llevado a cabo por personas que no son responsables por el objeto auditado.
- **NOTA 5:** una auditoría interna puede ser para la revisión por la dirección y otros propósitos internos y puede ser la base para la declaración de conformidad de una organización. La independencia puede ser demostrada mediante la no responsabilidad por la actividad que está siendo auditada. Las auditorías externas incluyen las de segunda y tercera parte. Las auditorías de segunda parte son realizadas por una parte que tiene un interés en la organización, como los clientes o por otras personas en su representación. Las auditorías de tercera parte son realizadas por organizaciones auditoras externas e independientes, como las que proveen la certificación o registro de conformidad o las agencias gubernamentales.
- **NOTA 6:** éste constituye uno de los términos comunes y las definiciones claves de la estructura de alto nivel de las normas de sistemas de gestión de ISO. La definición original fue modificada con la adición delas Notas a la entrada 4 y 5.

3.3 Continuidad del Negocio

Capacidad de la organización para continuar con la entrega de productos o servicios en un marco de tiempo aceptable a niveles predefinidos aceptables durante un incidente disruptivo.

[Fuente: ISO 22300:2018, 3.24 modificado- Esta definición ha sido reemplazada]

3.4 Plan de Continuidad del Negocio

Información documentada que guía a una organización para responder a un incidente disruptivo y recuperar, reanudar y restaurar la entrega de productos y servicios en forma coherente con sus objetivos de continuidad del negocio

[Fuente: ISO 22300:2018, 3.27 modificado- La definición ha sido reemplazada y la nota 1 a la entrada ha sido eliminada]

3.5 Análisis del Impacto en el Negocio

Proceso de análisis de impacto en el tiempo de un incidente disruptivo en la organización.

- **NOTA 1:** el resultado es una declaración y justificación de los requisitos (3.28) de continuidad del negocio (3.3).

[Fuente: ISO 22300:2018, 3.29 modificado. La definición ha sido reemplazada y la Nota 1 a la entrada ha sido añadida)]

3.6 Competencia

Capacidad de aplicar conocimientos y habilidades para alcanzar los resultados previstos.

- **NOTA 1:** Éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.7 Conformidad

Cumplimiento de un requisito.

- **Nota 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.8 Mejora Continua

Actividad recurrente para mejorar el desempeño.

- **NOTA 1**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.9 Acción Correctiva

Acción para eliminar las causas de una no conformidad y para prevenir la recurrencia.

- **NOTA 1**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.10 Incidente Disruptivo

Incidente anticipado o no anticipado, que causa una desviación no planificada y negativa de la entrega esperada de productos o servicios de acuerdo a los objetivos de una organización.

[Fuente: ISO 22300:2018, 3.70 modificado. La definición ha sido reemplazada.]

3.11 Información Documentada

Información que requiere ser controlada y mantenida por una organización (3.219 y el medio en que está contenida.

- **NOTA 1:** la información documentada puede estar en cualquier formato y medio y puede ser de cualquier fuente.
- **NOTA 2:** la información documentada se puede referir a:
  - El sistema de gestión, incluyendo los procesos relacionados.
  - La información creada para la operación de la organización (documentación).
  - La evidencia de los resultados logrados (registros).
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.12 Eficacia

Grado en que se realizan las actividades planificadas y se alcanzan los resultados planificados.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.13 Impacto

Resultado de un incidente disruptivo afectando a los objetivos.

[Fuente: ISO 22300:2018, 3.107 modificado. La definición ha sido reemplazada.]

3.14 Incidente

Evento que puede ser o puede dar lugar a un incidente disruptivo, pérdida, emergencia o crisis.

[Fuente: ISO 22300:2018, 3.111 modificado. La definición ha sido reemplazada.]

3.15 Partes Interesadas

Persona u organización que puede afectar, ser afectada, o percibirse a sí misma como afectada por una decisión o actividad.

Ejemplo: Los clientes, propietarios, personal, proveedores, bancos, reguladores, uniones, socios y la sociedad que puede incluir competidores o grupos opositores de presión.

- **NOTA 1:** una parte interesada puede ser un tomador de decisiones.
- **NOTA 2:** se consideran partes interesadas las comunidades afectadas o las poblaciones locales.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO. Se ha modificado la definición original con el agregado de un ejemplo y las Notas 1 y 2 a la entrada.

3.16 Sistema de Gestión

Conjunto de elementos interrelacionados o que interactúan, de una organización para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

- **NOTA 1:** un sistema de gestión puede abordar una o varias disciplinas.
- **NOTA 2:** los elementos del sistema incluyen la estructura de la organización, los roles y responsabilidades, la planificación, operación, etc.
- **NOTA 3:** el alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones a través de un grupo de organizaciones.
- **NOTA 4:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.17 Medición

Proceso para determinar un valor.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.18 Seguimiento

Determinar el estado de un sistema, un proceso o una actividad.

- **NOTA 1:** para determinar el estado puede haber una necesidad de comprobar, supervisar u observar críticamente.
- **NOTA 2:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.19 No Conformidad

Incumplimiento de un requisito.

- **NOTA 1**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.20 Objetivo

Resultado a ser logrado.

- **NOTA 1**: un objetivo puede ser estratégico, táctico u operacional.
- **NOTA 2:** los objetivos se pueden relacionar con diferentes disciplinas (tales como objetivos financieros, de la salud y la seguridad, y ambientales) y pueden aplicarse a diferentes niveles (tales como, estratégico, en toda la organización, proyecto, producto y proceso.
- **NOTA 3**: un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado deseado, un propósito, un criterio operacional, como una continuidad del negocio o por el uso de otras palabras de significado similar (por ejemplo, objetivo general , meta o aspiración).
- **NOTA 4:** en el contexto de las normas de sistemas de gestión de continuidad del negocio, los objetivos de continuidad del negocio son establecidos por la organización, en coherencia con la política (3.24) de continuidad del negocio, para lograr resultados específicos.
- **NOTA 5**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.21 Organización

Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

- **NOTA 1**: el concepto de organización incluye, pero no se limita a, compañía, corporación, firma, empresa, autoridad, asociación, empresa unipersonal, caridad o institución, o parte o combinación de los mismos, ya sean incorporadas o no, públicas o privadas.
- **NOTA 2:** para las organizaciones con más de un equipo de operación, una sola unidad operativa puede definirse como una organización.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO. La definición original fue modificada con el agregado de la Nota 2 a la entrada.

3.22 Subcontratar

Convenir un arreglo en el cual una organización externa realice parte de los procesos o funciones de una organización.

- **NOTA 1**: una organización externa está fuera del alcance del sistema de gestión aunque la función o el proceso externalizado estén dentro del alcance.
- **NOTA 2**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.23 Desempeño

Resultado medible.

- **NOTA 1:** el desempeño puede relacionarse con resultados cuantitativos o cualitativos.
- **NOTA 2:** el desempeño puede relacionarse con la gestión de actividades, procesos productos (incluidos los servicios), sistemas u organizaciones.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.24 Política

Intenciones y dirección de una organización como ha sido expresado formalmente por la alta dirección de la organización.

- **NOTA 1:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.25 Actividad Prioritaria

Actividad (3.1) a la que se le debe tratar con urgencia para evitar los impactos (3.13) no aceptables para el negocio durante un incidente disruptivo.

[Fuente: ISO 22300:2018, 3.176, modificada- La definición ha sido reemplazada y la Nota 1 a la entrada ha sido eliminada.]

3.26 Proceso

Conjunto de actividades (3.1) interrelacionadas o que interactúan, las cuales transforman elementos de entrada en salidas

- **NOTA 1**: éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.27 Productos y Servicios

Salidas o resultados proporcionados por una organización a sus partes interesadas.

- **NOTA 1**: por ejemplo los artículos manufacturados, seguros de automóviles y enfermería comunitaria.

[Fuente: ISO 22300:2018, 3.181, modificada- La definición ha sido reemplazada.]

3.28 Requisito

Necesidad o expectativa establecida, generalmente implícita u obligatoria.

- **NOTA 1:** organización y las partes interesadas que la necesidad o expectativa bajo consideración esté implícita.
- **NOTA 2**: un requisito especificado es uno que está establecido, por ejemplo, en la información documentada.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

3.29 Recursos

Todos los activos, personas, habilidades, información, tecnología (incluidas la planta física y los equipos), las instalaciones, y los suministros e información (ya sea electrónica o no) que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con sus objetivos.

[Fuente: ISO 22300:2018, 3.193, modificada- La definición ha sido reemplazada.]

3.30 Riesgo

Efecto de la incertidumbre sobre los objetivos (3.20).

- **NOTA 1**: un efecto es una desviación de lo esperado: positivo o negativo.
- **NOTA 2**: la incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con, entendimiento o conocimiento de un evento, su consecuencia o probabilidad.
- **NOTA 3**: el riesgo a menudo se caracteriza por la referencia a potenciales "eventos" (como se define en la Guía ISO 73) y "consecuencias" (como se define en la Guía ISO 73), o una combinación de estos.
- **NOTA 4**: el riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad de ocurrencia asociada (como se define en la Guía ISO 73).
- **NOTA 5**: esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO. La definición ha sido modificada para agregar "sobre los objetivos" para ser consistente con la norma ISO 31000.

3.31 Alta Dirección

Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.

- **NOTA 1**: la alta dirección tiene la facultad de delegar la autoridad y de proporcionar los recursos dentro de la organización.
- **NOTA 2**: si el alcance del sistema de gestión sólo cubre una parte de la organización, entonces, la alta dirección se orienta a los que dirigen y controlan esa parte de la organización.
- **NOTA 3:** éste constituye uno de los términos comunes y las definiciones clave de la estructura de alto nivel de las normas de sistemas de gestión de ISO.

ISO 22301 FOUNDATION (I22301F)

CertiProf®

Professional Knowledge

certiprof.com @Certiprof @CertiProf CertiProf Certiprof_llc

www.certiprof.com