

# INTERNACIONAL ESTÁNDAR

YO ASI  
**22301**

Segunda edición  
2019-10

---

---

## **Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos**

*Sécurité et résilience — Systèmes de management de la continuité  
d'activité — Exigencias*



Número de referencia  
ISO 22301:2019(E)

©ISO 2019



**DOCUMENTO PROTEGIDO POR DERECHOS DE AUTOR**

© ISO 2019

Reservados todos los derechos. A menos que se especifique lo contrario, o se requiera en el contexto de su implementación, ninguna parte de esta publicación puede ser reproducida o utilizada de ninguna forma o por ningún medio, electrónico o mecánico, incluidas las fotocopias, o la publicación en Internet o en una intranet, sin previo aviso. permiso escrito. El permiso se puede solicitar a ISO en la dirección que se indica a continuación o al organismo miembro de ISO en el país del solicitante.

oficina de derechos de autor ISO

CP 401 • Cap. de Blandonnet 8

CH-1214 Vernier, Ginebra

Teléfono: +41 22 749 01 11 Fax:

+41 22 749 09 47

Correo electrónico: [copyright@iso.org](mailto:copyright@iso.org)

Sitio web: [www.iso.org](http://www.iso.org)

Publicado en Suiza

# Contenido

Página

<b>Prefacio</b>	<b>v</b>
<b>Introducción</b>	<b>vi</b>
<b>1 Alcance</b>	<b>1</b>
<b>2 Referencias normativas</b>	<b>1</b>
<b>3 Términos y definiciones</b>	<b>1</b>
<b>4 Contexto de la organización</b>	<b>7</b>
4.1 Entender la organización y su contexto	7
4.2 Comprender las necesidades y expectativas de las partes interesadas	7
4.2.1 Generalidades	7
4.2.2 Requisitos legales y reglamentarios	7
4.3 Determinación del alcance del sistema de gestión de la continuidad del negocio	7
4.3.1 Generalidades	7
4.3.2 Alcance del sistema de gestión de la continuidad del negocio	8
4.4 Sistema de gestión de la continuidad del negocio	8
<b>5 Liderazgo</b>	<b>8</b>
5.1 Liderazgo y compromiso	8
5.2 Política	8
5.2.1 Establecimiento de la política de continuidad del negocio	8
5.2.2 Comunicación de la política de continuidad del negocio	9
5.3 Funciones, responsabilidades y autoridades	9
<b>6 Planificación</b>	<b>9</b>
6.1 Acciones para abordar riesgos y oportunidades	9
6.1.1 Determinación de riesgos y oportunidades	9
6.1.2 Abordar riesgos y oportunidades	9
6.2 Objetivos de continuidad del negocio y planificación para alcanzarlos	9
6.2.1 Establecimiento de objetivos de continuidad del negocio	9
6.2.2 Determinación de los objetivos de continuidad del negocio	10
6.3 Planificación de cambios en el sistema de gestión de continuidad del negocio	10
<b>7 Apoyo</b>	<b>10</b>
7.1 Recursos	10
7.2 Competencia	10
7.3 Conciencia	11
7.4 Comunicación	11
7.5 Información documentada	11
7.5.1 Generalidades	11
7.5.2 Creación y actualización	11
7.5.3 Control de la información documentada	12
<b>8 Operación</b>	<b>12</b>
8.1 Planificación y control operativo	12
8.2 Análisis de impacto empresarial y evaluación de riesgos	12
8.2.1 Generalidades	12
8.2.2 Análisis de impacto comercial	13
8.2.3 Evaluación de riesgos	13
8.3 Estrategias y soluciones de continuidad del negocio	13
8.3.1 Generalidades	13
8.3.2 Identificación de estrategias y soluciones	13
8.3.3 Selección de estrategias y soluciones	14
8.3.4 Necesidades de recursos	14
8.3.5 Implementación de soluciones	14
8.4 Planes y procedimientos de continuidad del negocio	14
8.4.1 Generalidades	14

	8.4.2 Estructura de respuesta.....	15
	8.4.3 Advertencia y comunicación.....	15
	8.4.4 Planes de continuidad del negocio.....	dieciséis
	8.4.5 Recuperación.....	17
	8.5 Programa de ejercicios.....	17
	8.6 Evaluación de la documentación y capacidades de continuidad del negocio.....	17
<b>9</b>	<b>Evaluación del desempeño.....</b>	<b>17</b>
	9.1 Seguimiento, medición, análisis y evaluación.....	17
	9.2 Auditoría interna.....	18
	9.2.1 Generalidades.....	18
	9.2.2 Programa(s) de auditoría.....	18
	9.3 Revisión por la dirección.....	18
	9.3.1 Generalidades.....	18
	9.3.2 Entrada de revisión de la dirección.....	18
	9.3.3 Resultados de la revisión por la dirección.....	19
<b>10</b>	<b>Mejora.....</b>	<b>19</b>
	10.1 No conformidad y acción correctiva.....	19
	10.2 Mejora continua.....	20
	<b>Bibliografía.....</b>	<b>21</b>

## Prefacio

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de Normas Internacionales normalmente se lleva a cabo a través de los comités técnicos de ISO. Cada organismo miembro interesado en un tema para el cual se ha establecido un comité técnico tiene derecho a estar representado en ese comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los asuntos de normalización electrotécnica.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en las Directivas ISO/IEC, Parte 1. En particular, se deben tener en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos ISO. Este documento fue redactado de acuerdo con las reglas editoriales de las Directivas ISO/IEC, Parte 2 (ver [www.iso.org/directivas](http://www.iso.org/directivas)).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan ser objeto de derechos de patente. ISO no será responsable de identificar cualquiera o todos los derechos de patente. Los detalles de cualquier derecho de patente identificado durante el desarrollo del documento estarán en la Introducción y/o en la lista ISO de declaraciones de patentes recibidas (ver [www.iso.org/patents](http://www.iso.org/patents)).

Cualquier nombre comercial utilizado en este documento es información proporcionada para la comodidad de los usuarios y no constituye un respaldo.

Para obtener una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicos de ISO relacionados con la evaluación de la conformidad, así como información sobre la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) en los obstáculos técnicos al comercio (TBT), consulte [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html).

Este documento fue preparado por el Comité Técnico ISO/TC 292, *Seguridad y resiliencia*.

Esta segunda edición anula y reemplaza la primera edición (ISO 22301:2012), que ha sido revisada técnicamente. Los principales cambios con respecto a la edición anterior son los siguientes:

- se han aplicado los requisitos de ISO para las normas de sistemas de gestión, que han evolucionado desde 2012;
- se han aclarado los requisitos, sin añadir nuevos requisitos;
- los requisitos de continuidad del negocio específicos de la disciplina ahora están casi completamente dentro [Cláusula 8](#);
- [Cláusula 8](#) se ha reestructurado para proporcionar una comprensión más clara de los requisitos clave;
- Se han modificado una serie de términos de continuidad del negocio específicos de la disciplina para mejorar la claridad y reflejar el pensamiento actual.

Cualquier comentario o pregunta sobre este documento debe dirigirse al organismo nacional de normalización del usuario. Una lista completa de estos organismos se puede encontrar en [www.iso.org/members.html](http://www.iso.org/members.html).

## Introducción

### 0.1 generales

Este documento especifica la estructura y los requisitos para implementar y mantener un sistema de gestión de la continuidad del negocio (BCMS) que desarrolle la continuidad del negocio adecuada a la cantidad y el tipo de impacto que la organización puede aceptar o no después de una interrupción.

Los resultados de mantener un BCMS están determinados por los requisitos legales, regulatorios, organizacionales y de la industria de la organización, los productos y servicios proporcionados, los procesos empleados, el tamaño y la estructura de la organización y los requisitos de sus partes interesadas.

Un BCMS enfatiza la importancia de:

- comprender las necesidades de la organización y la necesidad de establecer políticas y objetivos de continuidad del negocio;
- operar y mantener procesos, capacidades y estructuras de respuesta para garantizar que la organización sobreviva a las interrupciones;
- monitorear y revisar el desempeño y la efectividad del BCMS;
- mejora continua basada en medidas cualitativas y cuantitativas.

Un BCMS, como cualquier otro sistema de gestión, incluye los siguientes componentes:

- a) una política;
- b) personas competentes con responsabilidades definidas;
- c) procesos de gestión relacionados con:
  - 1) política;
  - 2) planificación;
  - 3) implementación y operación;
  - 4) evaluación del desempeño;
  - 5) revisión de la gestión;
  - 6) mejora continua;
- d) información documentada que apoye el control operativo y permita la evaluación del desempeño.

### 0.2 Beneficios de un sistema de gestión de continuidad del negocio

El propósito de un BCMS es preparar, proporcionar y mantener controles y capacidades para administrar la capacidad general de una organización para continuar operando durante las interrupciones. Para lograr esto, la organización es:

- a) desde una perspectiva comercial:
  - 1) apoyar sus objetivos estratégicos;
  - 2) crear una ventaja competitiva;
  - 3) proteger y mejorar su reputación y credibilidad;

- 4) contribuir a la resiliencia organizacional;
- b) desde una perspectiva financiera:
  - 1) reducir la exposición legal y financiera;
  - 2) reducir los costos directos e indirectos de las interrupciones;
- c) desde la perspectiva de las partes interesadas:
  - 1) proteger la vida, la propiedad y el medio ambiente;
  - 2) considerando las expectativas de las partes interesadas;
  - 3) proporcionar confianza en la capacidad de la organización para tener éxito;
- d) desde la perspectiva de los procesos internos:
  - 1) mejorar su capacidad para permanecer efectivo durante las interrupciones;
  - 2) demostrar un control proactivo de los riesgos de manera eficaz y eficiente;
  - 3) abordar las vulnerabilidades operativas.

### 0.3 Ciclo Planificar-Hacer-Verificar-Actuar (PDCA)

Este documento aplica el ciclo Planificar (establecer), Hacer (implementar y operar), Verificar (supervisar y revisar) y Actuar (mantener y mejorar) (PDCA) para implementar, mantener y mejorar continuamente la eficacia del BCMS de una organización.

Esto garantiza un grado de coherencia con otras normas de sistemas de gestión, como ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 e ISO 28000, lo que respalda una implementación y operación coherente e integrada con los sistemas de gestión relacionados.

De acuerdo con el ciclo PDCA, [Cláusulas 4 a 10](#) cubrir los siguientes componentes.

- [Cláusula 4](#) introduce los requisitos necesarios para establecer el contexto del BCMS aplicable a la organización, así como las necesidades, requisitos y alcance.
- [Cláusula 5](#) resume los requisitos específicos del rol de la alta dirección en el BCMS y cómo el liderazgo articula sus expectativas a la organización a través de una declaración de política.
- [Cláusula 6](#) describe los requisitos para establecer objetivos estratégicos y principios rectores para el BCMS en su conjunto.
- [Cláusula 7](#) apoya las operaciones de BCMS relacionadas con el establecimiento de competencia y comunicación de forma recurrente/según sea necesario con las partes interesadas, mientras se documenta, controla, mantiene y conserva la información documentada requerida.
- [Cláusula 8](#) define las necesidades de continuidad del negocio, determina cómo abordarlas y desarrolla procedimientos para gestionar la organización durante una interrupción.
- [Cláusula 9](#) resume los requisitos necesarios para medir el rendimiento de la continuidad del negocio, la conformidad del BCMS con este documento y para realizar la revisión de la dirección.
- [Cláusula 10](#) identifica y actúa sobre la no conformidad de BCMS y la mejora continua a través de acciones correctivas.

### 0.5 Contenido de este documento

Este documento cumple con los requisitos de ISO para los estándares de sistemas de gestión. Estos requisitos incluyen una estructura de alto nivel, texto central idéntico y términos comunes con definiciones centrales, diseñados para beneficiar a los usuarios que implementan múltiples estándares de sistemas de gestión ISO.

Este documento no incluye requisitos específicos de otros sistemas de gestión, aunque sus elementos pueden alinearse o integrarse con los de otros sistemas de gestión.

Este documento contiene requisitos que puede utilizar una organización para implementar un BCMS y evaluar la conformidad. Una organización que desee demostrar conformidad con este documento puede hacerlo mediante:

- realizar una autodeterminación y una autodeclaración; o
- solicitar la confirmación de su conformidad por partes que tengan un interés en la organización, como los clientes; o
- solicitar la confirmación de su autodeclaración por parte de una parte externa a la organización; o
- solicitar la certificación/registro de su BCMS por parte de una organización externa.

[Cláusulas 1 a 3](#) en este documento se establece el alcance, las referencias normativas y los términos y definiciones que se aplican al uso de este documento. [Cláusulas 4 a 10](#) contienen los requisitos que se utilizarán para evaluar la conformidad con este documento.

En este documento, se utilizan las siguientes formas verbales:

- a) “deberá” indica un requisito;
- b) “debería” indica una recomendación;
- c) “puede” indica un permiso;
- d) “can” indica una posibilidad o una capacidad.

La información marcada como “NOTA” es una guía para comprender o aclarar el requisito asociado. “Notas a la entrada” utilizadas en [Cláusula 3](#) proporcionar información adicional que complementa los datos terminológicos y puede contener disposiciones relativas al uso de un término.



# Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos

## 1 Alcance

Este documento especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger contra, reducir la probabilidad de que ocurra, prepararse para, responder y recuperarse de las interrupciones cuando surjan.

Los requisitos especificados en este documento son genéricos y están destinados a ser aplicables a todas las organizaciones, o partes de ellas, independientemente del tipo, tamaño y naturaleza de la organización. El alcance de la aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.

Este documento es aplicable a todos los tipos y tamaños de organizaciones que:

- a) implementar, mantener y mejorar un BCMS;
- b) tratar de garantizar la conformidad con la política de continuidad del negocio establecida;
- c) necesitan poder continuar entregando productos y servicios a una capacidad predefinida aceptable durante una interrupción;
- d) buscar mejorar su resiliencia a través de la aplicación efectiva del BCMS.

Este documento se puede utilizar para evaluar la capacidad de una organización para satisfacer sus propias necesidades y obligaciones de continuidad del negocio.

## 2 Referencias normativas

Los siguientes documentos se mencionan en el texto de tal manera que parte o la totalidad de su contenido constituye requisitos de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento de referencia (incluidas las modificaciones).

ISO 22300, *Seguridad y resiliencia — Vocabulario*

## 3 Términos y definiciones

A los efectos de este documento, se aplican los términos y definiciones proporcionados en ISO 22300 y los siguientes.

ISO e IEC mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones:

— Plataforma de navegación ISO Online: disponible en <https://www.iso.org/obp>

— Electropedia IEC: disponible en <http://www.electropedia.org/>

NOTA Los términos y definiciones que se dan a continuación reemplazan a los que se dan en la norma ISO 22300:2018.

### 3.1

#### actividad

conjunto de una o más tareas con un resultado definido

[ORIGEN: ISO 22300:2018, 3.1, modificado — Se reemplazó la definición y se eliminó el ejemplo.]

## 3.2

### auditoría

sistemático, independiente y documentado *proceso* (3.26) para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría

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

Nota 2 a la entrada: Una auditoría interna es realizada por el *organización* (3.21) por sí mismo, o por una parte externa en su nombre.

Nota 3 a la entrada: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

Nota 4 a la entrada: Los elementos fundamentales de una auditoría incluyen la determinación de la *conformidad* (3.7) de un objeto según un procedimiento llevado a cabo por personal que no es responsable del objeto auditado.

Nota 5 a la entrada: Una auditoría interna puede ser para revisión por la dirección y otros fines internos y puede formar la base para la declaración de conformidad de una organización. La independencia puede ser demostrada por la libertad de responsabilidad por el *actividad* (3.1) siendo auditado. Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte son realizadas por partes que tienen un interés en la organización, como los clientes, o por otras personas en su nombre. Las auditorías de terceros son realizadas por organizaciones de auditoría externas e independientes, como aquellas que brindan certificación/registro de conformidad o agencias gubernamentales.

Nota 6 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original se ha modificado agregando las Notas 4 y 5 a la entrada.

## 3.3

### continuidad del negocio

capacidad de un *organización* (3.21) para continuar la entrega de *productos y servicios* (3.27) dentro de marcos de tiempo aceptables a una capacidad predefinida durante un *ruptura* (3.10)

[FUENTE: ISO 22300:2018, 3.24, modificado — La definición ha sido reemplazada.]

## 3.4

### plan de negocios continuo

*información documentada* (3.11) que guía un *organización* (3.21) para responder a una *ruptura* (3.10) y reanudar, recuperar y restaurar la entrega de *productos y servicios* (3.27) consistente con su *continuidad del negocio* (3.3) *objetivos* (3.20)

[ORIGEN: ISO 22300:2018, 3.27, modificada — Se reemplazó la definición y se eliminó la Nota 1 a la entrada.]

## 3.5

### Análisis de Impacto del Negocio

*proceso* (3.26) de analizar la *impacto* (3.13) con el tiempo de un *ruptura* (3.10) sobre el *organización* (3.21)

Nota 1 a la entrada: El resultado es una declaración y justificación de *continuidad del negocio* (3.3) *requisitos* (3.28).

[ORIGEN: ISO 22300:2018, 3.29, modificada — Se reemplazó la definición y se agregó la Nota 1 a la entrada.]

## 3.6

### competencia

capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

## 3.7

### conformidad

cumplimiento de un *requisito* (3.28)

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**3.8****mejora continua**

periódico *actividad* (3.1) para mejorar *actuación* (3.23)

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**3.9****acción correctiva**

acción para eliminar la(s) causa(s) de una *disconformidad* (3.19) y para prevenir la recurrencia

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**3.10****ruptura**

*incidente* (3.14), ya sea anticipado o no anticipado, que cause una desviación negativa no planificada de la entrega esperada de *productos y servicios* (3.27) según un *de la organización* (3.21) *objetivos* (3.20)

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

**3.11****información documentada**

información requerida para ser controlada y mantenida por un *organización* (3.21) y el medio en el que está contenido

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

Nota 2 a la entrada: La información documentada puede referirse a:

- el *sistema de gestión* (3.16), incluidos los relacionados *procesos* (3.26);
- información creada para que la organización funcione (documentación);
- pruebas de los resultados obtenidos (registros).

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**3.12****eficacia**

medida en que se planeó *actividades* (3.1) se realizan y se logran los resultados planificados

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**3.13****impacto**

resultado de una *ruptura* (3.10) afectando *objetivos* (3.20)

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

**3.14****incidente**

evento que puede ser, o podría conducir a, una *ruptura* (3.10), pérdida, emergencia o crisis

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

### 3.15

#### **parte interesada (término preferido)**

parte interesada (término admitido)

persona o *organización* (3.21) que puede afectar, verse afectado o percibirse afectado por una decisión o *actividad* (3.1)

**EJEMPLO** Clientes, dueños, personal, proveedores, banqueros, reguladores, gremios, socios o sociedad que puede incluir competidores o grupos de presión opuestos.

Nota 1 a la entrada: Un tomador de decisiones puede ser una parte interesada.

Nota 2 a la entrada: Las comunidades afectadas y las poblaciones locales se consideran partes interesadas.

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original se ha modificado agregando 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* (3.21) para establecer *políticas* (3.24) y *objetivos* (3.20) y *procesos* (3.26) para lograr esos objetivos

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

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

Nota 3 a la entrada: 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 en un grupo de organizaciones.

Nota 4 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.17

#### **medición**

*proceso* (3.26) para determinar un valor

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.18

#### **supervisión**

determinar el estado de un sistema, un *proceso* (3.26) o una *actividad* (3.1)

Nota 1 a la entrada: Para determinar el estado, puede ser necesario verificar, supervisar u observar críticamente.

Nota 2 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.19

#### **disconformidad**

incumplimiento de un *requisito* (3.28)

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.20

#### **objetivo**

resultado a lograr

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

Nota 2 a la entrada: Los objetivos pueden relacionarse con diferentes disciplinas (como metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, de toda la organización, de proyecto, de producto y proceso(3.26)).

Nota 3 a la entrada: Un objetivo puede expresarse de otras formas, por ejemplo, como un resultado esperado, un propósito, un criterio operativo, como un*continuidad del negocio*(3.3) objetivo, o por el uso de otras palabras con un significado similar (por ejemplo, objetivo, meta o blanco).

Nota 4 a la entrada: En el contexto de la continuidad del negocio*sistemas de gestión*(3.16), los objetivos de continuidad del negocio son establecidos por el*organización*(3.21), en consonancia con la continuidad del negocio*política*(3.24), para lograr resultados específicos.

Nota 5 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.21

#### organización

persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr su*objetivos*(3.20)

Nota 1 a la entrada: El concepto de organización incluye, pero no se limita a, comerciante único, compañía, corporación, firma, empresa, autoridad, sociedad, caridad o institución, o parte o combinación de las mismas, ya sea incorporada o no, pública o privado.

Nota 2 a la entrada: Para organizaciones con más de una unidad operativa, una sola unidad operativa puede definirse como una organización.

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original ha sido modificada agregando la Nota 2 a la entrada.

### 3.22

#### subcontratar

hacer un arreglo donde un externo*organización*(3.21) realiza parte de la función de una organización o proceso(3.26)

Nota 1 a la entrada: Una organización externa está fuera del alcance de la*sistema de gestión*(3.16), aunque la función o proceso subcontratado está dentro del alcance.

Nota 2 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.23

#### actuación

resultado medible

Nota 1 a la entrada: El desempeño puede relacionarse con hallazgos cuantitativos o cualitativos.

Nota 2 a la entrada: El desempeño puede relacionarse con la gestión*actividades*(3.1),*procesos*(3.26), productos (incluidos los servicios), sistemas o*organizaciones*(3.21).

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.24

#### política

intenciones y dirección de un*organización*(3.21), tal como lo expresa formalmente su*alta dirección*(3.31)

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.25

#### actividad prioritaria

*actividad*([3.1](#)) a los que se da urgencia para evitar inaceptables *impactos*([3.13](#)) al negocio durante *unruptura*([3.10](#))

[ORIGEN: ISO 22300:2018, 3.176, modificado — Se reemplazó la definición y se eliminó la Nota 1 a la entrada.]

### 3.26

#### proceso

conjunto de elementos interrelacionados o que interactúan *actividades*([3.1](#)) que transforma entradas en salidas

Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.27

#### producto y servicio

producto o resultado proporcionado por una *organización*([3.21](#)) a *partes interesadas*([3.15](#))

EJEMPLO Artículos manufacturados, seguros de automóviles, enfermería comunitaria.

[FUENTE: ISO 22300:2018, 3.181, modificado: el término "producto y servicio" ha reemplazado a "producto o servicio" y la definición ha sido reemplazada.]

### 3.28

#### requisito

necesidad o expectativa declarada, generalmente implícita u obligatoria

Nota 1 a la entrada: "Generalmente implícito" significa que es costumbre o práctica común para una *organización*([3.21](#)) y *partes interesadas*([3.15](#)) que la necesidad o expectativa bajo consideración está implícita.

Nota 2 a la entrada: Un requisito especificado es uno que se establece, por ejemplo, en *información documentada*([3.11](#)).

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

### 3.29

#### recurso

todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones y suministros e información (ya sea electrónica o no) que una *organización*([3.21](#)) tiene que tener disponible para usar, cuando sea necesario, con el fin de operar y cumplir con sus *objetivos*([3.20](#))

[FUENTE: ISO 22300:2018, 3.193, modificado — La definición ha sido reemplazada.]

### 3.30

#### riesgo

efecto de la incertidumbre sobre *objetivos*([3.20](#))

Nota 1 a la entrada: Un efecto es una desviación de lo esperado, ya sea positivo o negativo.

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

Nota 3 a la entrada: El riesgo a menudo se caracteriza por referencia a posibles "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 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluidos los cambios en las circunstancias) y la probabilidad asociada (tal como se define en la Guía ISO 73) de ocurrencia.

Nota 5 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición se ha modificado para agregar "en los objetivos" para que sea coherente con la norma ISO 31000.

**3.31****alta dirección**

persona o grupo de personas que dirige y controla una *organización* (3.21) al más alto nivel

Nota 1 a la entrada: La alta dirección tiene el poder de delegar autoridad y proporcionar *recursos* (3.29) dentro de la organización.

Nota 2 a la entrada: Si el alcance de la *sistema de gestión* (3.16) cubre solo una parte de una organización, entonces la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización.

Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas del sistema de gestión ISO.

**4 Contexto de la organización****4.1 Entender la organización y su contexto**

La organización debe determinar los problemas externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados esperados de su BCMS.

NOTA Estos temas estarán influenciados por los objetivos generales de la organización, sus productos y servicios y la cantidad y tipo de riesgo que puede o no tomar.

**4.2 Comprender las necesidades y expectativas de las partes interesadas****4.2.1 Generalidades**

Al establecer su BCMS, la organización debe determinar:

- a) las partes interesadas que son relevantes para el BCMS;
- b) los requisitos pertinentes de estas partes interesadas.

**4.2.2 Requisitos legales y reglamentarios**

La organización deberá:

- a) implementar y mantener un proceso para identificar, tener acceso y evaluar los requisitos legales y reglamentarios aplicables relacionados con la continuidad de sus productos y servicios, actividades y recursos;
- b) asegurarse de que estos requisitos legales, reglamentarios y de otro tipo aplicables se tengan en cuenta al implementar y mantener su BCMS;
- c) documentar esta información y mantenerla actualizada.

**4.3 Determinación del alcance del sistema de gestión de la continuidad del negocio****4.3.1 Generalidades**

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

Al determinar este alcance, la organización debe considerar:

- a) las cuestiones externas e internas a que se refiere el 4.1 ;
- b) los requisitos a que se refiere el 4.2 ;
- c) su misión, fines y obligaciones internas y externas.

El alcance debe estar disponible como información documentada.

### 4.3.2 Alcance del sistema de gestión de la continuidad del negocio

La organización deberá:

- a) establecer las partes de la organización que se incluirán en el BCMS, teniendo en cuenta su(s) ubicación(es), tamaño, naturaleza y complejidad;
- b) identificar los productos y servicios que se incluirán en el BCMS.

Al definir el alcance, la organización debe documentar y explicar las exclusiones. No afectarán la capacidad y la responsabilidad de la organización para proporcionar continuidad del negocio, según lo determinado por el análisis de impacto en el negocio o la evaluación de riesgos y los requisitos legales o reglamentarios aplicables.

### 4.4 Sistema de gestión de la continuidad del negocio

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

## 5 Liderazgo

### 5.1 Liderazgo y compromiso

La alta dirección deberá demostrar liderazgo y compromiso con respecto al BCMS mediante:

- a) asegurar que la política de continuidad del negocio y los objetivos de continuidad del negocio estén establecidos y sean compatibles con la dirección estratégica de la organización;
- b) asegurar la integración de los requisitos del BCMS en los procesos de negocio de la organización;
- c) asegurar que los recursos necesarios para el BCMS estén disponibles;
- d) comunicar la importancia de la continuidad efectiva del negocio y de cumplir con los requisitos del BCMS;
- e) garantizar que el BCMS logre los resultados previstos;
- f) dirigir y apoyar a las personas para que contribuyan a la eficacia del BCMS;
- g) promover la mejora continua;
- h) apoyar a otros roles gerenciales relevantes para demostrar su liderazgo y compromiso en lo que se refiere a sus áreas de responsabilidad.

**NOTA** La referencia a “negocios” en este documento puede interpretarse en sentido amplio para referirse a aquellas actividades que son esencial para los propósitos de la existencia de la organización.

### 5.2 Política

#### 5.2.1 Establecimiento de la política de continuidad del negocio

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

- a) es apropiado para el propósito de la organización;
- b) proporciona un marco para establecer objetivos de continuidad del negocio;
- c) incluye un compromiso de satisfacer los requisitos aplicables;



d) incluye un compromiso de mejora continua del BCMS.

### 5.2.2 Comunicación de la política de continuidad del negocio

La política de continuidad del negocio deberá:

- a) estar disponible como información documentada;
- b) ser comunicado dentro de la organización;
- c) estar a disposición de los interesados, según corresponda.

### 5.3 Funciones, responsabilidades y autoridades

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

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) asegurar que el BCMS cumpla con los requisitos de este documento;
- b) informar sobre el desempeño del BCMS a la alta dirección.

## 6 Planificación

### 6.1 Acciones para abordar riesgos y oportunidades

#### 6.1.1 Determinación de riesgos y oportunidades

Al planificar el BCMS, la organización debe tener en cuenta las cuestiones a las que se hace referencia en [4.1](#) y los requisitos a que se refiere el [4.2](#) y determinar los riesgos y oportunidades que deben abordarse para:

- a) dar seguridad de que el BCMS puede lograr los resultados previstos;
- b) prevenir o reducir los efectos no deseados;
- c) lograr la mejora continua.

#### 6.1.2 Abordar riesgos y oportunidades

La organización debe planificar:

- a) acciones para abordar estos riesgos y oportunidades;
- b) cómo:
  - 1) integrar e implementar las acciones en sus procesos BCMS (ver [8.1](#));
  - 2) evaluar la efectividad de estas acciones (ver [9.1](#)).

NOTA Los riesgos y oportunidades se relacionan con la eficacia del sistema de gestión. Riesgos relacionados con interrupción del negocio se abordan en [8.2](#).

### 6.2 Objetivos de continuidad del negocio y planificación para alcanzarlos

#### 6.2.1 Establecimiento de objetivos de continuidad del negocio

La organización debe establecer objetivos de continuidad del negocio en las funciones y niveles pertinentes.

Los objetivos de continuidad del negocio deberán:

- a) ser consistente con la política de continuidad del negocio;
- b) ser medible (si es factible);
- c) tener en cuenta los requisitos aplicables (ver [4.1](#) y [4.2](#));
- d) ser monitoreado;
- e) ser comunicado;
- f) actualizarse según corresponda.

La organización debe conservar 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) lo que se hará;
- b) qué recursos se requerirán;
- c) quién será responsable;
- d) cuándo se completará;
- e) cómo se evaluarán los resultados.

### 6.3 Planificación de cambios en el sistema de gestión de continuidad del negocio

Cuando la organización determina la necesidad de cambios en el BCMS, incluidos los identificados en [Cláusula 10](#), los cambios se llevarán a cabo de manera planificada.

La organización deberá considerar:

- a) el propósito de los cambios y sus posibles consecuencias;
- b) la integridad del BCMS;
- c) la disponibilidad de recursos;
- d) la asignación o reasignación de responsabilidades y autoridades.

## 7 Soporte

### 7.1 Recursos

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

### 7.2 Competencia

La organización deberá:

- a) determinar la competencia necesaria de la(s) persona(s) que realizan el trabajo bajo su control que afecta el desempeño de la continuidad del negocio;
- b) garantizar que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas;

- c) en su caso, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas;
- d) conservar la información documentada apropiada como evidencia de competencia.

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

### 7.3 Conciencia

Las personas que realicen trabajos bajo el control de la organización deberán ser conscientes de:

- a) la política de continuidad del negocio;
- b) su contribución a la eficacia del BCMS, incluidos los beneficios de un mejor desempeño de la continuidad del negocio;
- c) las implicaciones de no cumplir con los requisitos del BCMS;
- d) su propio rol y responsabilidades antes, durante y después de las interrupciones.

### 7.4 Comunicación

La organización debe determinar las comunicaciones internas y externas relevantes para el BCMS, que incluyen:

- a) sobre lo que comunicará;
- b) cuándo comunicar;
- c) con quién comunicarse;
- d) cómo comunicarse;
- e) quién se comunicará.

### 7.5 Información documentada

#### 7.5.1 Generalidades

El BCMS de la organización debe incluir:

- a) información documentada requerida por este documento;
- b) información documentada determinada por la organización como necesaria para la eficacia del BCMS.

NOTA El alcance de la información documentada para un BCMS puede diferir 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;
- la competencia de las personas.

#### 7.5.2 Creación y actualización

Al crear y actualizar la información documentada, la organización debe garantizar lo siguiente:

- a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);
- b) formato (p. ej., idioma, versión de software, gráficos) y soporte (p. ej., papel, electrónico);

c) revisión y aprobación de la idoneidad y adecuación.

### **7.5.3 Control de la información documentada**

**7.5.3.1** La información documentada requerida por el BCMS y por este documento se controlará para asegurar:

- a) está disponible y es adecuado para su uso, donde y cuando se necesite;
- b) está adecuadamente protegido (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de 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 conservación, incluida la conservación de la legibilidad;
- c) control de cambios (por ejemplo, control de versiones);
- d) retención y disposición.

La información documentada de origen externo determinada por la organización como necesaria para la planificación y operación del BCMS debe identificarse, según corresponda, y controlarse.

**NOTA** El acceso puede implicar una decisión con respecto al permiso para ver únicamente la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada.

## **8 Operación**

### **8.1 Planificación y control operativo**

La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en [6.1](#), por:

- a) establecer criterios para los procesos;
- b) implementar el control de los procesos de acuerdo con los criterios;
- c) mantener la información documentada en la medida necesaria para tener confianza en que los procesos se han llevado a cabo según lo planeado.

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

La organización debe asegurarse de que los procesos subcontratados y la cadena de suministro estén controlados.

### **8.2 Análisis de impacto empresarial y evaluación de riesgos**

#### **8.2.1 Generalidades**

La organización deberá:

- a) implementar y mantener procesos sistemáticos para analizar el impacto comercial y evaluar los riesgos de interrupción;
- b) revisar el análisis de impacto en el negocio y la evaluación de riesgos a intervalos planificados y cuando haya cambios significativos dentro de la organización o el contexto en el que opera.

**NOTA** La organización determina el orden en que se realizan el análisis de impacto empresarial y la evaluación de riesgos. realizado.

### 8.2.2 Análisis de impacto comercial

La organización debe utilizar el proceso de análisis de los impactos en el negocio para determinar las prioridades y los requisitos de continuidad del negocio. El proceso deberá:

- a) definir los tipos de impacto y los criterios relevantes para el contexto de la organización;
- b) identificar las actividades que apoyan la provisión de productos y servicios;
- c) utilizar los tipos y criterios de impacto para evaluar los impactos a lo largo del tiempo resultantes de la interrupción de estas actividades;
- d) identificar el marco de tiempo dentro del cual los impactos de no reanudar las actividades serían inaceptables para la organización;

NOTA 1 Este período de tiempo puede denominarse "período máximo tolerable de interrupción (MTPD)".

- e) establecer marcos de tiempo priorizados dentro del tiempo identificado en d) para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada;

NOTA 2 Este marco de tiempo puede denominarse "objetivo de tiempo de recuperación (RTO)".

- f) utilizar este análisis para identificar actividades prioritarias;
- g) determinar qué recursos se necesitan para apoyar las actividades priorizadas;
- h) determinar las dependencias, incluidos socios y proveedores, e interdependencias de las actividades priorizadas.

### 8.2.3 Evaluación de riesgos

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

NOTA El proceso de evaluación de riesgos se aborda en la norma ISO 31000.

La organización deberá:

- a) identificar los riesgos de interrupción de las actividades prioritarias de la organización y de los recursos necesarios;
- b) analizar y evaluar los riesgos identificados;
- c) determinar qué riesgos requieren tratamiento.

NOTA Los riesgos en esta subcláusula se relacionan con la interrupción de las actividades comerciales. Riesgos y oportunidades relacionados a la eficacia del sistema de gestión se abordan en [6.1](#).

## 8.3 Estrategias y soluciones de continuidad del negocio

### 8.3.1 Generalidades

Con base en los resultados del análisis de impacto comercial y la evaluación de riesgos, la organización debe identificar y seleccionar estrategias de continuidad comercial que consideren opciones para antes, durante y después de la interrupción. Las estrategias de continuidad del negocio estarán compuestas por una o más soluciones.

### 8.3.2 Identificación de estrategias y soluciones

La identificación se basará en la medida en que las estrategias y soluciones:

- a) cumplir con los requisitos para continuar y recuperar las actividades priorizadas dentro de los plazos identificados y la capacidad acordada;

- b) proteger las actividades prioritarias de la organización;
- c) reducir la probabilidad de interrupción;
- d) acortar el período de interrupción;
- e) limitar el impacto de la interrupción en los productos y servicios de la organización;
- f) prever la disponibilidad de recursos adecuados.

### **8.3.3 Selección de estrategias y soluciones**

La selección se basará en la medida en que las estrategias y soluciones:

- a) cumplir con los requisitos para continuar y recuperar las actividades priorizadas dentro de los plazos identificados y la capacidad acordada;
- b) considerar la cantidad y el tipo de riesgo que la organización puede o no asumir;
- c) considerar los costos y beneficios asociados.

### **8.3.4 Necesidades de recursos**

La organización debe determinar los requisitos de recursos para implementar las soluciones de continuidad del negocio seleccionadas. Los tipos de recursos considerados incluirán, pero no se limitarán a:

- una personas;
- b) información y datos;
- c) infraestructura física como edificios, lugares de trabajo u otras instalaciones y servicios públicos asociados;
- d) equipos y consumibles;
- e) sistemas de tecnología de la información y la comunicación (TIC);
- f) transporte y logística;
- g) finanzas;
- h) socios y proveedores.

### **8.3.5 Implementación de soluciones**

La organización debe implementar y mantener soluciones de continuidad del negocio seleccionadas para que puedan activarse 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 permita alertas y comunicaciones oportunas a las partes interesadas relevantes. Debe proporcionar planes y procedimientos para gestionar la organización durante una interrupción. Los planes y procedimientos se utilizarán cuando sea necesario para activar las soluciones de continuidad del negocio.

**NOTA** Existen diferentes tipos de procedimientos que componen los planes de continuidad del negocio.

La organización debe identificar y documentar los planes y procedimientos de continuidad del negocio en función del resultado de las estrategias y soluciones seleccionadas.

Los procedimientos deberán:

- a) ser específico con respecto a los pasos inmediatos que deben tomarse durante una interrupción;
- b) ser flexible para responder a las cambiantes condiciones internas y externas de una interrupción;
- c) centrarse en el impacto de los incidentes que potencialmente conducen a una interrupción;
- d) ser efectivos en minimizar el impacto a través de la implementación de soluciones apropiadas;
- e) asignar roles y responsabilidades para las tareas dentro de ellos.

#### **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 responder a las interrupciones.

**8.4.2.2** Las funciones y responsabilidades de cada equipo y las relaciones entre los equipos deberán estar claramente establecidas.

**8.4.2.3** Colectivamente, los equipos serán competentes para:

- a) evaluar la naturaleza y el alcance de una interrupción y su impacto potencial;
- b) evaluar el impacto frente a umbrales predefinidos que justifiquen el inicio de una respuesta formal;
- c) activar una respuesta apropiada de continuidad del negocio;
- d) planificar las acciones que deben emprenderse;
- e) establecer prioridades (usando la seguridad de la vida como primera prioridad);
- f) monitorear los efectos de la interrupción 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 de comunicación.

**8.4.2.4** Para cada equipo habrá:

- a) personal identificado y sus suplentes con la responsabilidad, autoridad y competencia necesarias para desempeñar su función designada;
- b) procedimientos documentados para guiar sus acciones (ver [8.4.4](#)), incluidos los de activación, operación, coordinación y comunicación de la respuesta.

#### **8.4.3 Advertencia y comunicación**

**8.4.3.1** La organización debe documentar y mantener procedimientos para:

- a) comunicar interna y externamente a las partes interesadas relevantes, incluido qué, cuándo, con quién y cómo comunicarse;

NOTA La organización puede documentar y mantener procedimientos sobre cómo y bajo qué circunstancias, la organización se comunica con los empleados y sus contactos de emergencia.

- b) recibir, documentar y responder a las comunicaciones de las partes interesadas, incluido cualquier sistema de asesoramiento de riesgos nacional o regional o equivalente;
- c) garantizar la disponibilidad de los medios de comunicación durante una interrupción;

- d) facilitar la comunicación estructurada con los servicios de emergencia;
- e) proporcionar detalles de la respuesta de los medios de comunicación de la organización después de un incidente, incluida una estrategia de comunicación;
- f) registrar los detalles de la interrupción, las acciones tomadas y las decisiones tomadas.

**8.4.3.2** Cuando corresponda, también se considerará e implementará lo siguiente:

- a) alertar a las partes interesadas potencialmente afectadas por una interrupción real o inminente;
- b) asegurar la coordinación y comunicación apropiadas entre múltiples organizaciones de respuesta.

Los procedimientos de advertencia y comunicación deben ejercerse como parte del programa de ejercicios de la organización descrito 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 proporcionar orientación e información para ayudar a los equipos a responder a una interrupción y ayudar a la organización con la respuesta y la recuperación.

**8.4.4.2** Colectivamente, los planes de continuidad del negocio deberán contener:

- a) detalles de las acciones que los equipos tomarán para:
  - 1) continuar o recuperar actividades priorizadas dentro de plazos predeterminados;
  - 2) monitorear el impacto de la interrupción y la respuesta de la organización a la misma;
- b) referencia a los umbrales y procesos predefinidos para activar la respuesta;
- c) procedimientos para permitir la entrega de productos y servicios a la capacidad acordada;
- d) detalles para gestionar las consecuencias inmediatas de una interrupción teniendo debidamente en cuenta:
  - 1) el bienestar de las personas;
  - 2) la prevención de más pérdidas o indisponibilidad de actividades prioritarias;
  - 3) el impacto sobre el medio ambiente.

**8.4.4.3** Cada plan deberá incluir:

- a) la finalidad, alcance y objetivos;
- b) las funciones y responsabilidades del equipo que implementará el plan;
- c) acciones para implementar las soluciones;
- d) información de apoyo necesaria para activar (incluidos los criterios de activación), operar, coordinar y comunicar las acciones del equipo;
- e) interdependencias internas y externas;
- f) las necesidades de recursos;
- g) los requisitos de información;
- h) un proceso para retirarse.

Cada plan deberá ser utilizable y estar disponible en el momento y lugar en que se requiera.



#### 8.4.5 Recuperación

La organización debe tener procesos documentados para restaurar y recuperar las actividades comerciales de las medidas temporales adoptadas durante y después de una interrupción.

### 8.5 Programa de ejercicios

La organización debe implementar y mantener un programa de ejercicio y prueba para validar a lo largo del tiempo la eficacia de sus estrategias y soluciones de continuidad del negocio.

La organización realizará ejercicios y pruebas que:

- a) son consistentes con sus objetivos de continuidad del negocio;
- b) se basan en escenarios apropiados que están bien planificados con fines y objetivos claramente definidos;
- c) desarrollar el trabajo en equipo, la competencia, la confianza y el conocimiento de quienes tienen roles que desempeñar en relación con las interrupciones;
- d) en su conjunto a lo largo del tiempo, validar sus estrategias y soluciones de continuidad del negocio;
- e) producir informes formales posteriores al ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras;
- f) se revisan en el contexto de la promoción de la mejora continua;
- g) se realizan a intervalos planificados y cuando hay cambios significativos dentro de la organización o el contexto en el que opera.

La organización debe actuar sobre los resultados de su ejercicio y prueba para implementar cambios y mejoras.

### 8.6 Evaluación de la documentación y capacidades de continuidad del negocio

La organización deberá:

- a) evaluar la idoneidad, adecuación y eficacia de su análisis de impacto empresarial, evaluación de riesgos, estrategias, soluciones, planes y procedimientos;
- b) realizar evaluaciones a través de revisiones, análisis, ejercicios, pruebas, informes posteriores al incidente y evaluaciones de desempeño;
- c) realizar evaluaciones de las capacidades de continuidad del negocio de los socios y proveedores relevantes;
- d) evaluar el cumplimiento de los requisitos legales y reglamentarios aplicables, las mejores prácticas de la industria y la conformidad con su propia política y objetivos de continuidad del negocio;
- e) actualizar la documentación y los procedimientos de manera oportuna.

Estas evaluaciones se realizarán a intervalos planificados, después de un incidente o activación, y cuando ocurran cambios significativos.

## 9 Evaluación del desempeño

### 9.1 Seguimiento, medición, análisis y evaluación

La organización determinará:

- a) lo que necesita ser monitoreado y medido;

b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos;

c) cuándo y quién realizará el seguimiento y la medición;

d) cuándo y por quién se analizarán y evaluarán 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 del BCMS y la eficacia del BCMS.

## **9.2 Auditoría interna**

### **9.2.1 Generalidades**

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el BCMS:

a) se ajusta a:

- 1) los requisitos propios de la organización para su BCMS;
- 2) los requisitos de este documento;

b) se implementa y mantiene de manera efectiva.

### **9.2.2 Programa(s) de auditoría**

La organización deberá:

- a) planificar, establecer, implementar y mantener uno o más programas de auditoría que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la presentación de informes, que deberán tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores;
- b) definir los criterios de auditoría y el alcance de cada auditoría;
- c) seleccionar auditores y realizar auditorías para garantizar la objetividad y la imparcialidad del proceso de auditoría;
- d) asegurar que los resultados de las auditorías sean informados a los gerentes relevantes;
- e) retener información documentada como evidencia de la implementación del programa o programas de auditoría y los resultados de la auditoría;
- f) asegurar que se tomen las acciones correctivas necesarias sin demora indebida para eliminar las no conformidades detectadas y sus causas;
- g) asegurar que las acciones de auditoría de seguimiento incluyan la verificación de las acciones tomadas y el informe de los resultados de la verificación.

## **9.3 Revisión por la dirección**

### **9.3.1 Generalidades**

La alta dirección debe revisar el BCMS de la organización, a intervalos planificados, para garantizar su idoneidad, adecuación y eficacia continuas.

### **9.3.2 Entrada de revisión de la dirección**

La revisión por la dirección incluirá la consideración de:

- a) el estado de las acciones de revisiones de gestión anteriores;

- b) cambios en cuestiones externas e internas que son relevantes para el BCMS;
- c) información sobre el desempeño del BCMS, incluidas las tendencias en:
  - 1) no conformidades y acciones correctivas;
  - 2) seguimiento y medición de los resultados de la evaluación;
  - 3) resultados de la auditoría;
- d) comentarios de las partes interesadas;
- e) la necesidad de cambios en el BCMS, incluida la política y los objetivos;
- f) procedimientos y recursos que podrían utilizarse en la organización para mejorar el desempeño y la eficacia del BCMS;
- g) información del análisis de impacto en el negocio y evaluación de riesgos;
- h) resultado de la evaluación de la documentación y capacidades de continuidad del negocio (ver [8.6](#));
- i) riesgos o problemas que no se abordaron adecuadamente en ninguna evaluación de riesgos anterior;
- j) lecciones aprendidas y acciones derivadas de cuasi accidentes e interrupciones;
- k) oportunidades de mejora continua.

### **9.3.3 Resultados de la revisión por la dirección**

**9.3.3.1** Los resultados de la revisión por la dirección incluirán decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambios en el BCMS para mejorar su eficiencia y eficacia, incluidos los siguientes:

- a) variaciones al alcance del BCMS;
- b) actualización del análisis de impacto en el negocio, evaluación de riesgos, estrategias y soluciones de continuidad del negocio y planes de continuidad del negocio;
- c) modificación de procedimientos y controles para responder a problemas internos o externos que puedan afectar al BCMS;
- d) cómo se medirá la eficacia de los controles.

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

- a) comunicar los resultados de la revisión por la dirección a las partes interesadas pertinentes;
- b) tomar las medidas apropiadas en relación con esos resultados.

## **10 Mejora**

### **10.1 No conformidad y acción correctiva**

**10.1.1** La organización debe determinar las oportunidades de mejora e implementar las acciones necesarias para lograr los resultados previstos de su BCMS.

**10.1.2** Cuando ocurre una no conformidad, la organización debe:

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

1) tomar acciones para controlarlo y corregirlo;

2) hacer frente a las consecuencias;

b) evaluar la necesidad de acción para eliminar la(s) causa(s) de la no conformidad, a fin de que no se repita u ocurra en otro lugar, mediante:

1) revisar la no conformidad;

2) determinar las causas de la no conformidad;

3) determinar si existen no conformidades similares o pueden ocurrir potencialmente;

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada;

e) hacer cambios al BCMS, si es necesario.

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:

a) la naturaleza de las no conformidades y cualquier acción posterior tomada;

b) los resultados de cualquier acción correctiva.

## **10.2 Mejora continua**

La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del BCMS, con base en medidas cualitativas y cuantitativas.

La organización deberá considerar los resultados del análisis y la evaluación, y los resultados de la revisión por la dirección, para determinar si existen necesidades u oportunidades, relacionadas con el negocio o con el BCMS, que deberán abordarse como parte de la mejora continua.

**NOTA** La organización puede utilizar los procesos del BCMS, como liderazgo, planificación y desempeño, evaluación, para lograr la mejora.

## Bibliografía

- [1] ISO 9001, *Sistemas de gestión de la calidad — Requisitos*
- [2] ISO 14001, *Sistemas de gestión ambiental — Requisitos con orientación para su uso*
- [3] ISO 19011, *Directrices para la auditoría de los sistemas de gestión*
- [4] ISO/CEI/TS 17021-6, *Evaluación de la conformidad. Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión. Parte 6: Requisitos de competencia para la auditoría y certificación de sistemas de gestión de la continuidad del negocio.*
- [5] ISO/CEI 20000-1, *Tecnología de la información. Gestión de servicios. Parte 1: Gestión de servicios. Requisitos del sistema*
- [6] ISO 22313, *Seguridad social — Sistemas de gestión de la continuidad del negocio — Orientación*
- [7] ISO 22316, *Seguridad y resiliencia — Resiliencia organizacional — Principios y atributos*
- [8] ISO/TS 22317, *Seguridad social — Sistemas de gestión de la continuidad del negocio — Directrices para el análisis de impacto empresarial (BIA)*
- [9] ISO/TS 22318, *Seguridad social — Sistemas de gestión de la continuidad del negocio — Directrices para la continuidad de la cadena de suministro*
- [10] ISO/TS 22330, *Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Directrices para las personas aspectos de la continuidad del negocio*
- [11] ISO/TS 22331, *Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Directrices para la estrategia de continuidad del negocio*
- [12] ISO/CEI 27001, *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información sistemas — Requisitos*
- [13] ISO/CEI 27031, *Tecnología de la información. Técnicas de seguridad. Directrices para la preparación de la tecnología de la información y las comunicaciones para la continuidad del negocio.*
- [14] ISO 28000, *Especificación de sistemas de gestión de seguridad para la cadena de suministro*
- [15] ISO 31000, *Gestión de riesgos — Directrices*
- [16] CEI 31010, *Gestión de riesgos — Técnicas de evaluación de riesgos*
- [17] Guía ISO 73, *Gestión de riesgos — Vocabulario*