SISTEMAS DE GESTIÓN DE CONTINUIDAD DE NEGOCIO REQUISITOS

TABLA DE CONTENIDO

PREFACIO

ISO (la Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en un tema para el que se haya 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 ese 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 previstos para su posterior mantenimiento se describen en las Directivas ISO / IEC, Parte 1. En particular, deben tenerse 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/directives).

Se llama la atención sobre la posibilidad que algunos elementos en este documento puedan estar sujetos a derechos de patente. ISO no será responsable de identificar alguno 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).

Cualquier nombre comercial utilizado en este documento es información proporcionada para la conveniencia 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 Obstáculos Técnicos al Comercio (OTC), consulte 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 sustituye la primera edición (ISO 22301:2012), que ha sido revisada técnicamente. Los principales cambios respecto a la edición anterior son los siguientes:

- Se han aplicado los requisitos de ISO para las normas del sistema 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 están ahora casi en su totalidad dentro de la Cláusula 8;
- La cláusula 8 se ha reestructurado para proporcionar una comprensión más clara de los requisitos clave;
- Se han modificado varios términos de continuidad empresarial 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. Puede encontrar una lista completa de estos organismos en www.iso.org/members.html.

INTRODUCCIÓN

0.1 General

Este documento especifica la estructura y los requisitos para implementar y mantener un sistema de gestión de continuidad del negocio (BCMS) que desarrolle la continuidad del negocio de acuerdo con 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, reglamentarios, organizativos 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 sobrevivirá a las interrupciones;
- Reallizar seguimiento y revisión del rendimiento y la eficacia del BCMS;
- La 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 por la dirección;
   6) Mejora continua;
d) información documentada que respalde el control operativo y que permita la evaluación del desempeño.

0.2 Beneficios de un sistema de gestión de la continuidad empresarial

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 podrá:

a) Desde una perspectiva empresarial:
   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) Considerar las expectativas de las partes interesadas;
   3) Brindar confianza en la capacidad de la organización para tener éxito;
d) Desde una perspectiva de procesos internos:
   1) Mejorar su capacidad para seguir siendo eficaz 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 (monitorear y revisar) y Actuar (mantener y mejorar) para implementar, mantener y mejorar continuamente la eficacia del BCMS de una organización. Esto asegura un grado de coherencia con otras normas de sistemas de gestión, tales como ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 e ISO 28000, lo que respalda la implementación y el funcionamiento coherentes e integrados con los sistemas de gestión relacionados.

De acuerdo con el ciclo PHVA, las cláusulas 4 a 10 cubren los siguientes componentes.

- La cláusula 4 introduce los requisitos necesarios para establecer el contexto del BCMS aplicable a la organización, así como las necesidades, requisitos y alcance.
- La 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.
- La cláusula 6 describe los requisitos para establecer objetivos estratégicos y principios rectores para el BCMS en su conjunto.

- La cláusula 7 respalda las operaciones del BCMS relacionadas con el establecimiento de la competencia y la comunicación de forma recurrente o según sea necesario con las partes interesadas, mientras se documenta, controla, mantiene y retiene la información documentada requerida.
- La cláusula 8 define las necesidades de continuidad del negocio, determina cómo abordarlas y desarrolla procedimientos para gestionar la organización durante una interrupción.
- La cláusula 9 resume los requisitos necesarios para medir el desempeño de la continuidad del negocio, la conformidad del BCMS con este documento y para realizar la revisión por la dirección.
- La Cláusula 10 identifica y actúa sobre la no conformidad del BCMS y la mejora continua a través de acciones correctivas.

0.5 Contenido de este documento

Este documento cumple con los requisitos de la ISO para los estándares del sistema de gestión. Estos requisitos incluyen una estructura de alto nivel, un texto básico idéntico y términos comunes con definiciones básicas, 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:

- La formulación de una autodeterminación y una autodeclaración; o
- La confirmación de su conformidad por parte de las partes interesadas en la organización, como los clientes; o
- La confirmación de su autodeclaración por una parte externa a la organización; o
- La certificación / registro de su BCMS por una organización externa.

Las cláusulas 1 a 3 de este documento establecen el alcance, las referencias normativas y los términos y definiciones que se aplican al uso de este documento. Las 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) "puede" indica una posibilidad o capacidad.

La información marcada como "NOTA" es una guía para comprender o aclarar el requisito asociado. Las “Notas de entrada” utilizadas en la Cláusula 3 proporcionan información adicional que complementa los datos terminológicos y pueden contener disposiciones relacionadas con el uso de un término.

SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

1 ALCANCE

Este documento especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse, reducir la probabilidad de que ocurran, prepararse, 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 las mismas, 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) Busquen implementar, mantener y mejorar un BCMS;
b) Tratan de asegurar la conformidad con la política de continuidad del negocio establecida;
c) Tengan la necesidad de poder continuar entregando productos y servicios a una capacidad predefinida aceptable durante una interrupción;
d) Buscan mejorar su resiliencia mediante 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 de negocio.

2 REFERENCIAS NORMATIVAS

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

ISO 22300, Seguridad y resiliencia - Vocabulario

3 TÉRMINOS Y DEFINICIONES

Para los propósitos de este documento, se aplican los términos y definiciones dados en ISO 22300 y los siguientes.

ISO e IEC mantienen bases de datos terminológicas para su uso en normalización en las siguientes direcciones:
- Plataforma de navegación ISO Online: disponible en https://www.iso.org/obp
- IEC Electropedia: disponible en http://www.electropedia.org/

NOTA Los términos y definiciones dados a continuación reemplazan a los dados en ISO 22300: 2018.

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 el ejemplo ha sido eliminado.]

3.2 Auditoría
Proceso (3.26) sistemático, independiente y documentado 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 o tercera parte), y puede ser una auditoría combinada (combinando dos o más disciplinas).
Nota 2 a la entrada: La propia organización (3.21) realiza una auditoría interna o una parte externa en su nombre.
Nota 3 a la entrada: "Evidencia de auditoría" y "criterios de auditoría" se definen en ISO 19011.
Nota 4 a la entrada: Los elementos fundamentales de una auditoría incluyen la determinación de la conformidad (3.7) de un objeto de acuerdo con 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 propósitos internos y puede constituir la base para la declaración de conformidad de una organización. La independencia se puede demostrar por la ausencia de responsabilidad por la actividad (3.1) que se audita. 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 clientes, o por otras personas en su nombre. Las auditorías de terceros son realizadas por organizaciones de auditoría externas e independientes, como las que proporcionan certificación / registro de conformidad o agencias gubernamentales.
Nota 6 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original se ha modificado añadiendo las notas 4 y 5 a la entrada.

3.3 Continuidad del negocio
Capacidad de una organización (3.21) para continuar la entrega de productos y servicios (3.27) dentro de marcos de tiempo aceptables según la capacidad predefinida durante una interrupción (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 a una organización (3.21) para responder a una interrupción (3.10) y reanudar, recuperar y restaurar la entrega de productos y servicios (3.27) según sus objetivos de continuidad del negocio (3.3) (3.20)
[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 de Impacto al Negocio
Proceso (3.26) de análisis del impacto (3.13) a lo largo del tiempo de una interrupción (3.10) en la organización (3.21)
Nota 1 a la entrada: El resultado es una declaración y una justificación de los requisitos de continuidad del negocio (3.3) (3.28).
[FUENTE: ISO 22300: 2018, 3.29, modificado - Se reemplazó la definición y se agregó la Nota 1 a la entrada.]

3.6 Competencia
Capacidad para aplicar conocimientos y habilidades para lograr los resultados previstos
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.8 Mejora continua
Actividad recurrente (3.1) para mejorar el desempeño (3.23)
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas 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 no conformidad (3.19) y para prevenir la recurrencia
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas 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 causa una desviación negativa no planificada de la entrega esperada de productos y servicios (3.27) de acuerdo con los objetivos (3.21) de una organización (3.20)
[FUENTE: ISO 22300: 2018, 3.70, modificado - La definición ha sido reemplazada.]

3.11 Información documentada
Información que una organización (3.21) debe controlar y mantener y el medio en el que está contenida
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 procesos relacionados (3.26);
- Información creada para que la organización funcione (documentación);
- Evidencia de los resultados obtenidos (registros).

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

3.12 Eficacia
Medida en que se realizan las actividades planificadas (3.1) y se logran los resultados planificados
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.13 Impacto
Resultado de una interrupción (3.10) que afecta a los 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 interrupción (3.10), pérdida, emergencia o crisis
[FUENTE: ISO 22300: 2018, 3.111, modificado - La definición ha sido reemplazada.]

3.15 Parte interesada (término preferido) / Accionista (término admitido)
Persona u organización (3.21) que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o actividad (3.1)
EJEMPLO: Clientes, propietarios, personal, proveedores, banqueros, reguladores, sindicatos, socios o sociedad que pueden 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original se modificó 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 de la organización, roles y responsabilidades, planificación y operación.
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 básicas 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 básicas 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.19 No conformidad
Incumplimiento de un requisito (3.28)
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.20 Objetivo
Resultado a alcanzar
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 (tales como metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como estratégico, en toda la organización, proyecto, producto y proceso (3.26)).

Nota 3 a la entrada: Un objetivo se puede expresar de otras formas, p. Ej. como un resultado previsto, un propósito, un criterio operativo, como un objetivo de continuidad del negocio (3.3), o mediante el uso de otras palabras con un significado similar (por ejemplo, objetivo, meta o meta).
Nota 4 a la entrada: En el contexto de los sistemas de gestión de la continuidad del negocio (3.16), los objetivos de continuidad del negocio los establece la organización (3.21), de conformidad con la política de continuidad del negocio (3.24), para lograr resultados específicos.
Nota 5 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.21 Organización
Persona o grupo de personas que tiene funciones propias con responsabilidades, autoridades y relaciones para lograr sus objetivos (3.20)
Nota 1 a la entrada: El concepto de organización incluye, pero no se limita a, comerciante individual, 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición original se ha modificado agregando la Nota 2 a la entrada.

3.22 Subcontratar
Arreglo en el que una organización externa (3.21) realiza parte de la función o proceso de una organización (3.26)
Nota 1 a la entrada: Una organización externa está fuera del alcance del 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.23 Desempeño
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 de actividades (3.1), procesos (3.26), productos (incluidos los servicios), sistemas u organizaciones (3.21).
Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.24 Política
Intenciones y dirección de una organización (3.21), expresadas formalmente por su alta dirección (3.31)
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

3.25 Actividad priorizada
Actividad (3.1) a la que se le da urgencia para evitar impactos inaceptables (3.13) en el negocio durante una interrupción (3.10)
[FUENTE: ISO 22300: 2018, 3.176, modificado - La definición ha sido reemplazada y la Nota 1 a la entrada ha sido eliminada.]

3.26 Proceso
Conjunto de actividades interrelacionadas o que interactúan (3.1) que transforman entradas en salidas
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones básicas 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 las partes interesadas (3.15)
EJEMPLO: Artículos manufacturados, seguro de automóvil, 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 que se declara, generalmente implícita u obligatoria
Nota 1 a la entrada: "Generalmente implícito" significa que es costumbre o práctica común para la organización (3.21) y las partes interesadas (3.15) que la necesidad o expectativa bajo consideración esté implícita.
Nota 2 a la entrada: Un requisito especificado es uno que se establece, p. Ej. en información documentada (3.11).
Nota 3 a la entrada: Este constituye uno de los términos comunes y definiciones básicas 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) debe tener disponible para usar, cuando sea necesario, para operar y cumplir con sus objetivo (3,20)
[FUENTE: ISO 22300: 2018, 3.193, modificado - La definición ha sido reemplazada.]

3.30 Riesgo
Efecto de la incertidumbre sobre los objetivos (3.20)
Nota 1 a la entrada: Un efecto es una desviación de lo esperado: positivo o negativo.
Nota 2 a la entrada: 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 se caracteriza a menudo 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 (como se define en la Guía ISO 73) de que ocurra.
Nota 5 a la entrada: Este constituye uno de los términos comunes y definiciones básicas de la estructura de alto nivel para las normas del sistema de gestión ISO. La definición ha sido modificada para agregar "sobre objetivos" para ser consistente con ISO 31000.

3.31 Alta gerencia
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) en la organización.
Nota 2 a la entrada: Si el alcance del 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 básicas de la estructura de alto nivel para las normas del sistema de gestión ISO.

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y su contexto

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

NOTA Estos problemas 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 Comprensión de las necesidades y expectativas de las partes interesadas

4.2.1 General

Al establecer su BCMS, la organización debe determinar:

a) Las partes interesadas que sean relevantes para el BCMS;
b) Los requisitos relevantes de estas partes interesadas.

4.2.2 Requisitos legales y reglamentarios

La organización debe:

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 General

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 mencionadas en 4.1;
b) Los requisitos mencionados en 4.2;
c) Su misión, metas 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 debe:

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 responsabilidad de la organización para proporcionar continuidad de negocio, según lo determinado por el análisis de impacto al 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 debe demostrar liderazgo y compromiso con respecto al BCMS al:

a) Asegurar que la política de continuidad del negocio y los objetivos de continuidad del negocio se establezcan 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 del negocio eficaz 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 contribuir a la eficacia del BCMS;
g) Promover la mejora continua;
h) Apoyar otros roles gerenciales relevantes para demostrar liderazgo y compromiso en lo referido a su área de responsabilidad.

NOTA La referencia a "negocios" en este documento se puede interpretar de manera amplia como aquellas actividades que son fundamentales 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) Sea apropiada para el propósito de la organización;
b) Proporcione un marco para establecer objetivos de continuidad del negocio;
c) Incluya el compromiso de satisfacer los requisitos aplicables;
d) Incluya un compromiso con la mejora continua del BCMS.

5.2.2 Comunicar la política de continuidad del negocio

La política de continuidad del negocio deberá:

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

5.3 Roles, responsabilidades y autoridades

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

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurarse de 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 considerar los problemas mencionados en 4.1 y los requisitos mencionados en 4.2 y determinar los riesgos y oportunidades que deben abordarse para:

a) Garantizar que el BCMS puede lograr los resultados previstos;
b) Prevenir o reducir efectos no deseados;
c) Lograr una mejora continua.

6.1.2 Abordar los riesgos y las 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 eficacia de estas acciones (ver 9.1).

NOTA Los riesgos y las oportunidades se relacionan con la eficacia del sistema de gestión. Los riesgos relacionados con la interrupción del negocio se tratan en 8.2.

6.2 Objetivos de continuidad del negocio y planificación para lograrlos

6.2.1 Establecimiento de objetivos de continuidad del negocio

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

Los objetivos de continuidad del negocio deberán:

a) Ser coherentes con la política de continuidad del negocio;
b) Ser medibles (si es factible);
c) Tener en cuenta los requisitos aplicables (ver 4.1 y 4.2);
d) Ser monitoreados;
e) Ser comunicados;
f) Actualizarse según corresponda.

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

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

Cuando la organización determina la necesidad de cambios en el BCMS, incluidos los identificados en la Cláusula 10, los cambios deben llevarse a cabo de manera planificada.

La organización debe 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 debe:

a) Determinar la competencia necesaria de la (s) persona (s) que realizan el trabajo bajo su control que afecta su desempeño en la continuidad del negocio;
b) Asegurarse de que estas personas sean competentes sobre la base de una educación, formación o experiencia adecuadas;
c) Cuando corresponda, tomar acciones para adquirir competencia necesaria y evaluar la eficacia de las acciones tomadas;
d) Conservar la información documentada adecuada como prueba de competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo, la provisión de capacitación, la tutoría o la reasignación 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 conocer:

a) La política de continuidad del negocio;
b) Su contribución a la eficacia del BCMS, incluidos los beneficios de un mejor desempeño en 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, incluyendo:

a) Sobre lo que comunicará;
b) Cuándo comunicarse;
c) Con quién comunicarse;
d) Cómo comunicarse;
e) Quién se comunicará..

7.5 Información documentada

7.5.1 General

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 información documentada, la organización debe asegurarse de que sea apropiado:

a) Identificación y descripción (por ejemplo, título, fecha, autor o número de referencia);
b) Formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico);
c) Revisión y aprobación de 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 debe controlarse para garantizar:

a) Que está disponible y es adecuada para su uso, donde y cuando se necesite;
b) Que está adecuadamente protegida (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 que la organización determine como necesaria para la planificación y operación del BCMS deberá identificarse, según corresponda, y controlarse.

NOTA El acceso puede implicar una decisión con respecto al permiso para ver solo 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 los requisitos y para implementar las acciones determinadas en 6.1, mediante:

a) El establecimiento de criterios para los procesos;
b) La implementación de controles en los procesos de acuerdo con los criterios;
c) El mantenimiento de 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 al negocio y evaluación de riesgos

8.2.1 General

La organización debe:

a) Implementar y mantener procesos sistemáticos para analizar el impacto al negocio y evaluar los riesgos de interrupción;
b) Revisar el análisis de impacto al negcio 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 el que se realizan el análisis de impacto al negocio y la evaluación de riesgos.

8.2.2 Análisis de impacto al negocio

La organización debe utilizar el proceso para analizar los impactos del 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 el impacto de no reanudar 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 plazo puede denominarse "objetivo de tiempo de recuperación (RTO)".
f) Utilizar este análisis para identificar actividades priorizadas;
g) Determinar qué recursos se necesitan para apoyar las actividades priorizadas;
h) Determinar las dependencias, incluyendo socios y proveedores, y las 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 ISO 31000.

La organización debe:

a) Identificar los riesgos de interrupción de las actividades priorizadas de la organización y de sus recursos requeridos;
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 de negocio. Los riesgos y oportunidades relacionados con la eficacia del sistema de gestión se tratan en 6.1.

8.3 Estrategias y soluciones de continuidad del negocio

8.3.1 General

Con base en los resultados del análisis de impacto al negocio y la evaluación de riesgos, la organización debe identificar y seleccionar estrategias de continuidad de negocio que consideren opciones 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 los requisitos para continuar y recuperar las actividades priorizadas en plazos identificados y capacidad acordada;
b) Proteger las actividades priorizadas de la organización;
c) Reducir la probabilidad de interrupciones;
d) Acortar el período de interrupción;
e) Limitar el impacto de la interrupción en los productos y servicios de la organización;
f) Asegurar 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 los requisitos para continuar y recuperar las actividades priorizadas en plazos identificados y la capacidad acordada;
b) Considerar la cantidad y el tipo de riesgo que la organización puede asumir o no;
c) Considerar 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 del negocio seleccionadas. Los tipos de recursos considerados incluirán, pero no se limitarán a:

a) 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 las comunicaciones (TIC);
f) Transporte y logística;
g) Finanzas;
h) Socios y proveedores.

8.3.5 Implementación de soluciones

La organización debe implementar y mantener las 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 General

La organización debe implementar y mantener una estructura de respuesta que permita advertencia y comunicación oportunas a las partes interesadas relevantes. Deberá proporcionar planes y procedimientos para gestionar la organización durante una interrupción. Los planes y procedimientos se utilizarán cuando sea necesario para activar soluciones de continuidad del negocio.
NOTA Existen diferentes tipos de procedimientos que comprenden los planes de continuidad del negocio.

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

Los procedimientos deberán:

a) Ser específicos con respecto a los pasos inmediatos que se deben tomar durante una interrupción;
b) Ser flexibles para responder a las cambiantes condiciones internas y externas de una interrupción;
c) Centrarse en el impacto de los incidentes que potencialmente conducen a interrupciones;
d) Ser eficaces para minimizar el impacto mediante la implementación de soluciones adecuadas;
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 Los roles y responsabilidades de cada equipo y las relaciones entre los equipos deben estar claramente establecidos.

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 justifican 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 (utilizando la seguridad humana 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 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 aquellos para la 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) Comunicarse interna y externamente con las partes interesadas pertinentes, incluido qué, cuándo, con quién y cómo;
   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 aviso de riesgos nacional o regional o equivalente;
c) Asegurar la disponibilidad de los medios de comunicación durante una interrupción;
d) Facilitar la comunicación estructurada con los servicios de emergencia;
e) Pproporcionar 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 debe considerar e implementar lo siguiente:

a) Alertar a las partes interesadas potencialmente afectadas por una interrupción real o inminente;
b) Asegurar una adecuada coordinación y comunicación entre múltiples organizaciones de respuesta.

Los procedimientos de advertencia y comunicación se deben aplicar 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 En conjunto, los planes de continuidad del negocio deben contener:

a) Detalles de las acciones que los equipos llevarán a cabo para:
   1) Dontinuar o recuperar actividades priorizadas dentro de marcos de tiempo predeterminados;
   2) Monitorear el impacto de la interrupción y la respuesta de la organización a ella;
b) Referencia a los umbrales predefinidos y al proceso 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 nuevas pérdidas o indisponibilidad de actividades priorizadas;
   3) El impacto sobre el medio ambiente.

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) 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) Los requisitos de recursos;
g) Los requisitos de información;
h) Un proceso de retirada.

Cada plan se podrá utilizar y estará disponible en el momento y lugar en que se requiera.

8.4.5 Recuperación

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

8.5 Programa de ejercicios y pruebas

La organización debe implementar y mantener un programa de ejercicios y pruebas para validar con el tiempo la eficacia de sus estrategias y soluciones de continuidad del negocio.

La organización debe realizar ejercicios y pruebas que:

a) Sean coherentes con sus objetivos de continuidad del negocio;
b) Basados en escenarios apropiados que están bien planificados con metas y objetivos claramente definidos;
c) Desarrollen el trabajo en equipo, la competencia, la confianza y el conocimiento para aquellos que tienen roles que desempeñar en relación con las interrupciones;
d) En conjunto, a lo largo del tiempo, validen sus estrategias y soluciones de continuidad del negocio;
e) Produzcan informes posteriores al ejercicio formalizados que contengan resultados, recomendaciones y acciones para implementar mejoras;
f) Se revisen en el contexto de la promoción de la mejora continua;
g) Se realicen 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 las capacidades de continuidad del negocio

La organización debe:

a) Evaluar la idoneidad, adecuación y eficacia de su análisis de impacto al negocio, 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, luego de un incidente o activación y ante cambios significativos.

9 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

La organización debe determinar:

a) Qué se necesita monitorear y medir;
b) Los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar resultados válidos;
c) Cuándo y quién debe realizar el seguimiento y la medición;
d) Cuándo y quién debe 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 del BCMS y la eficacia del BCMS.

9.2 Auditoría interna

9.2.1 General

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

a) Se ajusta a:
   1) Los propios requisitos 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 debe:

a) Planificar, establecer, implementar y mantener un programa o 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 las auditorías anteriores;
b) Definir los criterios de auditoría y el alcance de cada auditoría;
c) Seleccionar auditores y realizar auditorías para asegurar la objetividad y la imparcialidad del proceso de auditoría;
d) Asegurarse de que los resultados de las auditorías se informen 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) Asegurarse de que se tomen las acciones correctivas necesarias sin demora indebida para eliminar las no conformidades detectadas y sus causas;
g) Asegurarse de 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 General

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

9.3.2 Entrada de la revisión por la dirección

La revisión por la dirección debe incluir la consideración de:

a) El estado de las acciones de las revisiones por la dirección anteriores;
b) Cambios en asuntos externos e internos 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 al negocio y evaluación de riesgos;
h) Resultado de la evaluación de la documentación y las capacidades de continuidad del negocio (ver 8.6);
i) Riesgos o problemas que no se abordan 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 deben incluir decisiones relacionadas con oportunidades de mejora continua y cualquier necesidad de cambios en el BCMS para mejorar su eficiencia y eficacia, incluyendo lo siguiente:

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

9.3.3.2 La organización debe retener 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 adecuadas en relación con esos resultados.

10 MEJORA

10.1 No conformidad y acción correctiva

10.1.1 La organización debe determinar 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 ante la no conformidad y, según corresponda:
   1) Tomar medidas para controlarlo y corregirlo;
   2) Lidiar con 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 ni ocurra en otro lugar, mediante:
   1) La revisión de la no conformidad;
   2) La determinación de las causas de la no conformidad;
   3) El determinar si existen no conformidades similares o si pueden ocurrir potencialmente;
c) Implementar cualquier acción necesaria;
d) Revisar la eficacia de cualquier acción correctiva tomada;
e) Realizar cambios en el BCMS, si es necesario.

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

10.1.3 La organización debe retener 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, basándose en medidas cualitativas y cuantitativas.

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

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

BIBLIOGRAFÍA

[1] ISO 9001, Quality management systems — Requirements
[2] ISO 14001, Environmental management systems — Requirements with guidance for use
[3] ISO 19011, Guidelines for auditing management systems
[4] ISO/IEC/TS 17021-6, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems
[5] ISO/IEC 20000-1, Information technology — Service management — Part 1: Service management system requirements
[6] ISO 22313, Societal security — Business continuity management systems — Guidance
[7] ISO 22316, Security and resilience — Organizational resilience — Principles and attributes
[8] ISO/TS 22317, Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)
[9] ISO/TS 22318, Societal security — Business continuity management systems — Guidelines for supply chain continuity
[10] ISO/TS 22330, Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity
[11] ISO/TS 22331, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
[12] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
[13] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
[14] ISO 28000, Specification for security management systems for the supply chain
[15] ISO 31000, Risk management — Guidelines
[16] IEC 31010, Risk management — Risk assessment techniques
[17] ISO Guide 73, Risk management — Vocabulary