NORMA TÉCNICA PERUANA

NTP-ISO 22301 2020

Dirección de Normalización - INACAL
Calle Las Camelias 817, San Isidro (Lima 27) Lima, Perú

Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. Requisitos

Security and resilience. Business continuity management systems. Requirements

(EQV. ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements)

2020-04-02
1ª Edición

R.D. N° 004-2020-INACAL/DN. Publicada el 2020-04-07 Precio basado en 40 páginas
I.C.S.: 03.100.01; 03.100.70 ESTA NORMA ES RECOMENDABLE
Descriptores: Seguridad, resiliencia, organización, gestión de la empresa, sistemas de gestión

INACAL

Calle Las Camelias 817, San Isidro
Lima - Perú
Tel.: +51 1 640-8820
publicaciones@inacal.gob.pe
www.inacal.gob.pe

ÍNDICE

PRÓLOGO

A. RESEÑA HISTÓRICA

A.1 El Instituto Nacional de Calidad - INACAL, a través de la Dirección de Normalización es la autoridad competente que aprueba las Normas Técnicas Peruanas a nivel nacional. Es miembro de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en representación del país.

A.2 La presente Norma Técnica Peruana ha sido elaborada por iniciativa de la Dirección de Normalización del Instituto Nacional de Calidad –INACAL, con base en el Acápite A.1 del artículo 19 del Reglamento de Elaboración y Aprobación de Normas Técnicas Peruanas, Guías y Textos Afines a las Actividades de Normalización, mediante el Sistema 1 o de Adopción, durante el mes de marzo de 2020, utilizando como antecedente a la norma ISO 22301:2019 Security and resilience - Business continuity management systems – Requirements.

A.3 La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:2016 y GP 002:2016.

PRÓLOGO
(ISO)

La 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 se lleva a cabo normalmente a través de comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se ha establecido un comité técnico, tiene el derecho a estar representado en dicho 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 todas las materias de normalización electrotécnica.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en la norma ISO/IEC Directivas, Parte 1. En particular, debe tenerse en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos ISO. Este documento fue elaborado de acuerdo con las normas editoriales de la IEC Directivas ISO/, parte 2 (véase www.iso.org/directives).

Se llama la atención a la posibilidad de que algunos de los elementos de este documento puede ser objeto de derechos de patente. ISO no se hace responsable de la identificación de cualquiera o todos los derechos de patente. Los detalles de cualquier derecho de patente identificados durante el desarrollo del documento estarán en la introducción y/o en la lista ISO de las declaraciones de patentes recibidas (véase www.iso.org/patents).

Cualquier nombre comercial utilizado en el presente documento se da información para la comodidad de los usuarios y no constituye un endoso.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos y expresiones específicas ISO relacionados con la evaluación de la conformidad, así como información acerca de la adherencia de ISO de los principios de la Organización Mundial del Comercio (OMC) en los obstáculos técnicos al comercio (OTC) véase www.iso.org/iso/foreword.html .

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

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

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

Cualquier comentario o consulta sobre este documento debería 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 Generalidades

En este documento se especifican la estructura y los requisitos para la implementación y el mantenimiento de un sistema de gestión de continuidad del negocio (SGCN) que desarrolle una continuidad del negocio adecuada a la cantidad y el tipo de impacto que la organización pueda o no aceptar tras una disrupción.

Los resultados del mantenimiento de un SGCN están conformados 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 SGCN enfatiza la importancia de:

- entender las necesidades de la organización y la necesidad por 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 disrupciones;
- supervisar y examinar el desempeño y la eficacia del SGCN; y
- la mejora continua basada en medidas cualitativas y cuantitativas.

Un SGCN, 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) la política;

2) la planificación;

3) la implementación y operación;

4) evaluación del desempeño;

5) revisión por la gerencia;

6) mejora continua; y

d) información documentada que apoye el control operacional y permita la evaluación del desempeño.

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

El propósito de un SGCN es preparar, proporcionar y mantener controles y capacidades para gestionar la capacidad general de una organización para seguir funcionando durante las disrupciones. Para lograr esto, la organización está:

a) desde una perspectiva empresarial:

1) apoyando sus objetivos estratégicos;

2) creando ventaja competitiva;

3) protegiendo y mejorando su reputación y credibilidad;

4) contribuyendo a la resistencia de la organización;

b) desde una perspectiva financiera:

1) reduciendo la exposición jurídica y financiera;

2) reduciendo los costos directos e indirectos de las disrupciones;

c) desde la perspectiva de las partes interesadas:

1) protegiendo la vida, la propiedad y el medio ambiente;

2) considerando las expectativas de las partes interesadas;

3) proporcionando confianza en la capacidad de la organización para tener éxito;

d) desde la perspectiva de los procesos internos:

1) mejorando su capacidad para seguir siendo eficaz durante las disrupciones;

2) demostrando un control proactivo de los riesgos de manera eficaz y eficiente; y

3) abordando las vulnerabilidades operacionales.

0.3 Ciclo Planificar-Hacer-Verificar-Actuar (PHVA)

Este documento aplica el ciclo Planificar (establecer), Hacer (y operar), Verificar (controlar y revisar) y Actuar (mantener y mejorar) (PHVA) para, mantener y mejorar continuamente la efectividad del SGCN de una organización.

Esto garantiza un grado de coherencia con otras normas de sistemas de gestión, como la ISO 9001, la ISO 14001, la ISO/IEC 20000-1, la ISO/IEC 27001 y la ISO 28000, apoyando así la aplicación y el funcionamiento coherentes e integrados con los sistemas de gestión relacionados.

De conformidad con el ciclo del PHVA, los capítulos 4 a 10 abarcan los siguientes componentes.

- El capítulo 4 introduce los requisitos necesarios para establecer el contexto del SGCN aplicable a la organización, así como las necesidades, los requisitos y el alcance.

- En el capítulo 5 se resumen los requisitos específicos del rol de la alta dirección en el SGCN, y la forma en que el liderazgo articula sus expectativas en la organización mediante una declaración de política.

- El capítulo 6 describe los requisitos para establecer los objetivos estratégicos y los principios rectores para el SGCN en su conjunto.

- El capítulo 7 apoya las operaciones del SGCN relacionadas con el establecimiento de la competencia y comunicación de forma recurrente o según sea necesario con las partes interesadas, a la vez que se documenta, controla, mantiene y conserva la información documentada requerida.

- El capítulo 8 define las necesidades de continuidad del negocio, determina cómo abordarlas y desarrolla procedimientos para gestionar la organización durante una disrupción. En el capítulo 9 se resumen los requisitos necesarios para medir el rendimiento de la continuidad del negocio, la conformidad del SGCN con este documento y la conducción de una revisión por la gerencia.

- El capítulo 10 identifica y actúa sobre la no conformidad y la mejora continua del SGCN mediante la adopción de medidas correctivas.

0.4 Contenido del presente documento

El presente documento se ajusta a los requisitos de la ISO en materia de normas de sistemas 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 normas de sistemas de gestión de la ISO.

El presente documento no incluye los 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 pueden ser utilizados por una organización para implementar un SGCN y evaluar su conformidad. Una organización que desee demostrar su conformidad con este documento puede hacerlo mediante:

- haciendo una autodeterminación y una autodeclaración; o
- buscando la confirmación de su conformidad por las partes que tienen un interés en la organización, como sus clientes; o
- buscando la confirmación de su autodeclaración por una parte externa a la organización; o
- buscando la certificación/registro de su SGCN por una organización externa.

Los capítulos 1 a 3 del presente documento establecen el alcance, las referencias normativas y los términos y definiciones que se aplican al utilizar del presente documento. Los capítulos 4 a 10 contienen los requisitos que se utilizarán para evaluar la conformidad con el presente documento.

En este documento se utilizan las siguientes formas verbales:

a) "debe" indica un requisito;

b) "debería" indica una recomendación;

c) "podría" indica un permiso; y

d) "puede" indica una posibilidad o una capacidad.

La información marcada como "NOTA" sirve de orientación para entender o clarificar el requisito asociado. Las "notas a la entrada" utilizadas en el capítulo 3 proporcionan información adicional que complementa los datos terminológicos y pueden contener disposiciones relativas al uso de un término.

---oooOooo---

Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. Requisitos

1 Objeto y campo de aplicación

Esta Norma Técnica Peruana especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para proteger, reducir la probabilidad de ocurrencia, prepararse para, responder a y recuperarse de disrupciones cuando estos surjan.

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

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

a) implementen, mantengan y mejoren un SGCN;

b) busquen garantizar la conformidad con la política de continuidad del negocio establecida;

c) necesiten ser capaces de continuar entregando productos y servicios a una capacidad aceptable previamente definida durante una disrupción; y

d) busquen mejorar su resiliencia a través de la aplicación efectiva del SGCN.

Esta Norma Técnica Peruana 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, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda).

ISO 22300 Seguridad y resiliencia — Vocabulario

3 Términos y definiciones

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

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

- Plataforma de navegación en línea ISO: disponible en https://www.iso.org/obp
- IEC Electropedia: disponible en http: //www.electropedia.org/

NOTA: Los términos y definiciones que figuran a continuación sustituyen a los que figuran en la norma ISO 22300.

3.1
actividad
conjunto de una o más tareas con una salida definida

[FUENTE: ISO 22300, 3.1 modificada- La definición ha sido reemplazada y el ejemplo ha sido eliminado.]

3.2
auditoría
proceso (véase subcapítulo 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 parte o tercera parte), y puede ser una auditoría combinada (que combina dos o más disciplinas).

Nota 2 a la entrada: La organización (véase subcapítulo 3.21) o una parte externa en su nombre conducen una auditoría interna.

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 (véase subcapítulo 3.7) de un objeto de acuerdo con un procedimiento llevado a cabo por el personal que no es responsable por el objeto auditado.

Nota 5 a la entrada: Una auditoría interna puede ser para revisión de la administración y otros propósitos internos y puede formar la base para la declaración de conformidad de una organización. La independencia puede ser demostrada mediante la libertad de responsabilidad de la actividad (véase subcapítulo 3.1) que se audita. Las auditorías externas incluyen auditorías de segunda y de tercera parte. Las auditorías de segunda parte son realizadas por partes interesadas en la organización, como clientes, o por otras personas en su nombre. Las auditorías de tercera parte son realizadas por organizaciones de auditoría externas e independientes, como las que proporcionan certificación/registro de conformidad o entidades gubernamentales.

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

3.3
continuidad del negocio
capacidad de una organización (véase subcapítulo 3.21) para continuar la entrega de productos y servicios (véase subcapítulo 3.27) dentro de plazos aceptables a una capacidad predefinida durante una disrupción (véase subcapítulo 3.10)

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

3.4
plan de continuidad del negocio
información documentada (véase subcapítulo 3.11) que guía a una organización (véase subcapítulo 3.21) para responder a una disrupción (véase subcapítulo 3.10) y reanudar, recuperar y restaurar la entrega de productos y servicios (véase subcapítulo 3.27) de acuerdo con sus objetivos (véase subcapítulo 3.20) de continuidad del negocio (véase subcapítulo 3.3)

[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 en el negocio
proceso (véase subcapítulo 3.26) de analizar el impacto (véase subcapítulo 3.13) sobre el periodo de tiempo de una disrupción (véase subcapítulo 3.10) en la organización (véase subcapítulo 3.21)

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

[FUENTE: ISO 22300:2018, 3.29, modificado - La definición ha sido reemplazada y se ha agregado 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: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO.

3.7
conformidad
cumplimiento de un requisito (véase subcapítulo 3.28)

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

3.8
mejora continua
actividad (véase subcapítulo 3.1) recurrente para mejorar el desempeño (véase subcapítulo 3.23)

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

3.9
acción correctiva
Acción para eliminar la (s) causa (s) de una no conformidad (véase subcapítulo 3.19) y para prevenir su recurrencia

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

3.10
disrupción
incidente (véase subcapítulo 3.14), ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios (véase subcapítulo 3.27) de acuerdo con los objetivos (véase subcapítulo 3.20) de una organización (véase subcapítulo 3.21)

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

3.11
información documentada
información requerida para ser controlada y mantenida por una organización (véase subcapítulo 3.21) y el medio en el que está contenida

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

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

- el sistema de gestión (véase subcapítulo 3.16), incluidos los procesos (véase subcapítulo 3.26) relacionados ;

- información creada para que la organización opere (documentación); y
- evidencia de resultados alcanzados (registros).

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

3.12
eficacia
extensión en que se realizan las actividades (véase subcapítulo 3.1) planificadas y se alcanzan los resultados planificados

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

3.13
impacto
resultado de una disrupción (véase subcapítulo 3.10) que afecta los objetivos (véase subcapítulo 3.20)

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

3.14
incidente
evento que puede ser o podría provocar una disrupción (véase subcapítulo 3.10), pérdida, emergencia o crisis

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

3.15
parte interesada (término preferido)
socio (término admitido)
persona u organización (véase subcapítulo 3.21) que puede afectar, verse afectada o percibirse así misma como afectada por una decisión o actividad (véase subcapítulo 3.1)

EJEMPLO: Clientes, propietarios, personal, proveedores, banqueros, reguladores, sindicatos, socios o sociedad que pueden incluir competidores o grupos opositores de presión.

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

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

Nota 3 a la entrada: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO. La definición original se ha modificado agregando un ejemplo y las Notas 1 y 2 a la entrada.

3.16
sistema de gestión
conjunto de elementos de una organización (véase subcapítulo 3.21) interrelacionados o que interactúan para establecer políticas (véase subcapítulo 3.24) y objetivos (véase subcapítulo 3.20) y procesos (véase subcapítulo 3.26) para alcanzar 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: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO.

3.17
medición
proceso (véase subcapítulo 3.26) para determinar un valor

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

3.18
seguimiento
determinar el estado de un sistema, un proceso (véase subcapítulo 3.26) o una actividad (véase subcapítulo 3.1)

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

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

3.19
no conformidad
no cumplimiento de un requisito (véase subcapítulo 3.28)

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

3.20
objetivo
resultado a ser alcanzado

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 a nivel estratégico, de toda la organización, proyecto, producto y proceso (véase subcapítulo 3.26)).

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

Nota 4 a la entrada: En el contexto de los sistemas de gestión (véase subcapítulo 3.16) de continuidad del negocio, la organización (véase subcapítulo 3.21) establece los objetivos de continuidad del negocio, de acuerdo con la política (véase subcapítulo 3.24) de continuidad del negocio, para lograr resultados específicos.

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

3.21
organización
persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridad y relaciones para lograr sus objetivos (véase subcapítulo 3.20)

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

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: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO. La definición original se ha modificado agregando la Nota 2 a la entrada.

3.22
subcontratar (outsource), verbo
hacer un arreglo donde una organización (véase subcapítulo 3.21) externa realiza parte de la función o proceso (véase subcapítulo 3.26) de una organización

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

Nota 2 a la entrada: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas 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 actividades (véase subcapítulo 3.1) de gestión, procesos (véase subcapítulo 3.26), productos (incluidos servicios), sistemas u organizaciones (véase subcapítulo 3.21).

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

3.24
política
intenciones y dirección de una organización (véase subcapítulo 3.21), expresada formalmente por su alta dirección (véase subcapítulo 3.31)

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

3.25
actividad priorizada
actividad (véase subcapítulo 3.1) a la que se le asigna un nivel de urgencia para evitar impactos (véase subcapítulo 3.13) inaceptables en el negocio durante una disrupción (véase subcapítulo 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 (véase subcapítulo 3.1) interrelacionadas o que interactúan que transforman las entradas en salidas

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

3.27
producto y servicio
salida o resultado proporcionado por una organización (véase subcapítulo 3.21) a las partes interesadas (véase subcapítulo 3.15)

EJEMPLO: Artículos manufacturados, seguros de automóviles, enfermería comunitaria.

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

3.28
requisito
necesidad o expectativa establecida, generalmente implícita u obligatoria

Nota 1 a la entrada: “Generalmente implícito” significa que es costumbre o práctica común para la organización (véase subcapítulo 3.21) y las partes interesadas (véase subcapítulo 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 (véase subcapítulo 3.11).

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

3.29
recurso
todos los activos (incluyendo planta y equipamiento), personas, habilidades, tecnología, instalaciones y suministros e información (ya sea electrónica o no) que una organización (véase subcapítulo 3.21) tiene que tener disponible para usar, cuando necesite, para operar y cumplir con su objetivo (véase subcapítulo 3.20)

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

3.30
riesgo
efecto de la incertidumbre sobre los objetivos (véase subcapítulo 3.20)

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

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

Nota 3 a la entrada: El riesgo a menudo se caracteriza por la referencia a potenciales "eventos" (como se define en la Guía ISO 73) y "consecuencias" (como se define en la Guía ISO 73), o una combinación de estos.

Nota 4 a la entrada: El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las circunstancias) y la probabilidad de ocurrencia asociada (como se define en la Guía ISO 73).

Nota 5 a la entrada: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO. La definición ha sido modificada para agregar "sobre los objetivos" para ser consistente con la norma ISO 31000.

3.31
alta dirección
persona o grupo de personas que dirige y controla una organización (véase subcapítulo 3.21) al más alto nivel

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

Nota 2 a la entrada: si el alcance del sistema de gestión (véase subcapítulo 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: Esto constituye uno de los términos comunes y definiciones centrales de la estructura de alto nivel para las normas de sistemas de gestión ISO.

4 Contexto de la organización

4.1 Comprensión de la organización y su contexto

La organización debe determinar las cuestiones externas e internas que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados previstos de su SGCN.

NOTA: Estas cuestiones estarán influenciadas por los objetivos generales de la organización, sus productos y servicios y la cantidad y tipo de riesgo que puede o no asumir.

4.2 Entender las necesidades y expectativas de las partes interesadas

4.2.1 Generalidades

Al establecer su SGCN, la organización debe determinar:

a) las partes interesadas que son relevantes para el SGCN; y

b) los requisitos relevantes de estas partes interesadas.

4.2.2 Requisitos legales y regulatorios

La organización debe:

a) implementar y mantener un proceso para identificar, tener acceso a, y evaluar los requisitos legales y regulatorios aplicables relacionados con la continuidad de sus productos y servicios, actividades y recursos;

b) garantizar que estos requisitos legales, regulatorios y de otro tipo se tomen en cuenta al implementar y mantener su SGCN;

c) documentar esta información y mantenerla actualizada.

4.3 Determinar el alcance del sistema de gestión de continuidad del negocio

4.3.1 Generalidades

La organización debe determinar los límites y la aplicabilidad del SGCN para establecer su alcance. Al determinar este alcance, la organización debe considerar:

a) las cuestiones externas e internas mencionadas en el subcapítulo 4.1;

b) los requisitos mencionados en el subcapítulo 4.2; y

c) su misión, objetivos y obligaciones internas y externas.

El alcance debe estar disponible como información documentada.

4.3.2 Alcance del sistema de gestión de continuidad del negocio

La organización debe:

a) establecer las partes de la organización que se incluirán en el SGCN, tomando en cuenta su localización(es), tamaño, naturaleza y complejidad; y

b) identificar productos y servicios a ser incluidos en el SGCN.

Al definir el alcance, la organización debe documentar y explicar las exclusiones. Estas no deben afectar la capacidad y la responsabilidad de la organización de 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 regulatorios aplicables.

4.4 Sistema de gestión de continuidad del negocio

La organización debe establecer, implementar, mantener y mejorar continuamente un SGCN, 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 SGCN al:

a) garantizar que la política y los objetivos de continuidad del negocio estén establecidos y sean compatibles con la dirección estratégica de la organización;

b) garantizar la integración de los requisitos del SGCN en los procesos de negocio de la organización;

c) garantizar que los recursos necesarios para el SGCN estén disponibles;

d) comunicar la importancia de una efectiva continuidad del negocio y la conforme con los requisitos del SGCN;

e) garantizar que el SGCN logre los resultados previstos;

f) dirigir y apoyar a las personas para que contribuyan a la efectividad del SGCN;

g) promover la mejora continua; y

h) apoyar otros roles gerenciales relevantes para demostrar su liderazgo y compromiso en lo que respecta a sus áreas de responsabilidad.

NOTA: La referencia a "negocio" en este documento puede interpretarse de manera amplia para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

5.2 Política

5.2.1 Establecer la política de continuidad del negocio

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

a) sea apropiada para el propósito de la organización;

b) proporcione un marco de referencia para establecer objetivos de continuidad del negocio;

c) incluya un compromiso para satisfacer los requisitos aplicables; y

d) incluya un compromiso de mejora continua del SGCN.

5.2.2 Comunicación de la política de continuidad del negocio

La política de continuidad del negocio debe:

a) estar disponible como información documentada;

b) ser comunicada dentro de la organización; y

c) estar disponible para las partes interesadas, según corresponda.

5.3 Roles, responsabilidades y autoridad

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

La alta dirección debe asignar la responsabilidad y la autoridad para:

a) asegurar que el SGCN sea conforme con los requisitos de este documento; y

b) informar sobre el desempeño del SGCN 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 SGCN, la organización debe considerar las cuestiones referidas en el subcapítulo 4.1 y los requisitos mencionados en el subcapítulo 4.2 y determinar los riesgos y oportunidades que necesitan abordarse para:

a) garantizar que el SGCN pueda lograr su(s) resultado(s) deseado(s);

b) prevenir o reducir los efectos no deseados; y

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 los procesos del SGCN (véase subcapítulo 8.1);

2) evaluar la eficacia de estas acciones (véase subcapítulo 9.1).

NOTA: Los riesgos y las oportunidades se relacionan con la eficacia del sistema de gestión. Los riesgos relacionados con disrupciones del negocio se abordan en el subcapítulo 8.2.

6.2 Objetivos de continuidad del negocio y planificación para alcanzarlos

6.2.1 Estableciendo los objetivos de continuidad del negocio

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

Los objetivos de continuidad del negocio deben:

a) ser coherentes con la política de continuidad del negocio;

b) ser medibles (si es posible);

c) tomar en cuenta los requisitos aplicables (véase subcapítulos 4.1 y 4.2);

d) ser sujetos de seguimiento;

e) ser comunicados; y

f) estar actualizados según corresponda.

La organización debe retener 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; y

e) cómo se evaluarán los resultados.

6.3 Planificando los cambios en el sistema de gestión de continuidad del negocio

Cuando la organización determina la necesidad de cambios en el SGCN, incluidos los identificados en el capítulo 10, los cambios se deben llevar a cabo de manera planificada.

La organización debe considerar:

a) el propósito de los cambios y sus consecuencias potenciales;

b) la integridad del SGCN;

c) la disponibilidad de recursos; y

d) la asignación o reasignación de responsabilidades y autoridad.

7 Soporte

7.1 Recursos

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

7.2 Competencia

La organización debe:

a) determinar la competencia necesaria de la(s) persona(s) que realiza(n) el trabajo bajo su control que afecta su desempeño de continuidad del negocio;

b) asegurar que estas personas sean competentes sobre la base de una educación, capacitación o experiencia apropiadas;

c) cuando corresponda, tomar medidas para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas; y

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

NOTA: Las acciones aplicables pueden incluir, por ejemplo, la provisión de entrenamiento, la tutoría o la reasignación de personas actualmente empleadas; o el reclutamiento o contratación de personas competentes.

7.3 Toma de conciencia

Las personas que trabajen bajo el control de la organización deben tener conciencia de:

a) la política de continuidad del negocio;

b) su contribución a la eficacia del SGCN, incluyendo los beneficios de un mejor desempeño de la continuidad del negocio;

c) las implicaciones de no cumplir con los requisitos del SGCN; y

d) su propio rol y responsabilidades antes, durante y después de las disrupciones.

7.4 Comunicación

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

a) lo que se comunicará;

b) cuándo comunicarlo;

c) a quién comunicarlo;

d) cómo comunicarlo; y

e) quién lo comunicará.

7.5 Información documentada

7.5.1 Generalidades

El SGCN de la organización debe incluir:

a) información documentada requerida por este documento; y

b) información documentada determinada como necesaria por la organización para la eficacia del SGCN.

NOTA: El alcance de la información documentada para un SGCN 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; y
- la competencia de las personas.

7.5.2 Creando y actualizando

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

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

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

c) la 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 SGCN y por este documento debe ser controlado para garantizar que:

a) está disponible y es adecuada para su uso, donde y cuando sea necesaria; y

b) 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 sea aplicable:

a) distribución, acceso, recuperación y uso;

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

c) control de cambios (por ejemplo, control de versiones); y

d) retención y disposición.

La información documentada de origen externo que la organización determine que es necesaria para la planificación y operación del SGCN debe ser identificada, según sea apropiada, y controlada.

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 operacional

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

a) estableciendo criterios para los procesos;

b) implementando el control de los procesos de acuerdo con los criterios; y

c) manteniendo la información documentada en la extensión necesaria para tener la confianza de 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 intencionados, tomando acciones para mitigar los efectos adversos, según sea necesario.

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

8.2 Análisis de impacto en el negocio y evaluación de riesgos

8.2.1 Generalidades

La organización debe:

a) implementar y mantener procesos sistemáticos para analizar el impacto en el negocio y evaluar los riesgos de disrupción; y

b) revisar el análisis de impacto en el negocio y la valoración 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 conducen el análisis de impacto en el negocio y la valoración de riesgos.

8.2.2 Análisis de impacto en el negocio

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

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 como resultado de la disrupción 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 plazo puede denominarse "período máximo de disrupción tolerable (MTPD, por sus siglas en inglés)".

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 " tiempo objetivo de recuperación (RTO, por sus siglas en inglés)".

f) utilizar este análisis para identificar actividades priorizadas;

g) determinar cuáles recursos son necesarios para apoyar actividades priorizadas; y

h) determinar las dependencias, incluidos los socios y proveedores, y las interdependencias de las actividades priorizadas.

8.2.3 Evaluación de riesgos

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

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

La organización debe:

a) identificar los riesgos de disrupción para las actividades priorizadas de la organización y de sus recursos requeridos;

b) analizar y evaluar los riesgos identificados; y

c) determinar cuáles riesgos requieren tratamiento.

NOTA: Los riesgos en este subcapítulo se relacionan con la disrupción de las actividades del negocio. Los riesgos y oportunidades relacionados con la efectividad del sistema de gestión se abordan en el subcapítulo 6.1.

8.3 Estrategias y soluciones de continuidad del negocio

8.3.1 Generalidades

Con base en los resultados del análisis de impacto en el negocio y la evaluación de riesgos, la organización debe identificar y seleccionar estrategias de continuidad del negocio que consideren opciones para antes, durante y después de la disrupción. Las estrategias de continuidad del negocio se deben conformar a partir de una o más soluciones.

8.3.2 Identificación de estrategias y soluciones

La identificación debe estar basada en la extensión en que las estrategias y soluciones:

a) cumplan con los requisitos para continuar y recuperar actividades priorizadas dentro de los plazos de tempo identificados y la capacidad acordada;

b) protejan las actividades priorizadas de la organización;

c) reduzcan la probabilidad de disrupción;

d) acorten el período de disrupción;

e) limiten el impacto de la disrupción sobre los productos y servicios de la organización; y

f) proporcionen la disponibilidad de recursos adecuados.

8.3.3 Selección de estrategias y soluciones

La selección debe estar basada en la extensión en que las estrategias y soluciones:

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

b) consideren la cantidad y el tipo de riesgo que la organización puede o no asumir; y

c) consideren 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 deben incluir, pero no estar limitados a:

a) personas;

b) información y datos;

c) infraestructura física como edificios, lugares de trabajo u otras instalaciones y servicios asociados;

d) equipamiento y consumibles;

e) sistemas de tecnología de la información y la comunicación (TIC);

f) transporte y logística;

g) finanzas; y

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 ser activadas cuando sea necesario.

8.4 Planes y procedimientos de continuidad del negocio

8.4.1 Generalidades

La organización debe implementar y mantener una estructura de respuesta que permita una advertencia (alerta) oportuna y comunicación a las partes interesadas relevantes. Esto debe proporcionar planes y procedimientos para gestionar a la organización durante una disrupción. Los planes y procedimientos deben ser utilizados cuando se requiera para activar soluciones de continuidad del negocio.

NOTA: Existen diferentes tipos de procedimientos que comprenden planes de continuidad del negocio.

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

Los procedimientos deben:

a) ser específicos con respecto a los pasos inmediatos a ser tomados durante una disrupción;

b) ser flexibles para responder a las condiciones cambiantes internas y externas de una disrupción;

c) centrarse en el impacto de los incidentes que potencialmente conducen a una disrupción;

d) ser eficaces para minimizar el impacto mediante la implementación de soluciones apropiadas; y

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 por responder a las disrupciones.

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

8.4.2.3 Colectivamente, los equipos deben ser competentes para:

a) evaluar la naturaleza y la extensión de una disrupción y su potencial impacto;

b) evaluar el impacto contra umbrales predefinidos que justifican el inicio de una respuesta formal;

c) activar una respuesta adecuada de continuidad del negocio;

d) planificar acciones que necesitan ser llevadas a cabo;

e) establecer prioridades (considerando como primera prioridad salvaguardar la vida);

f) monitorear los efectos de la disrupción y la respuesta de la organización;

g) activar las soluciones de continuidad del negocio; y

h) comunicarse con las partes interesadas relevantes, la autoridad y los medios.

8.4.2.4 Para cada equipo debe existir:

a) personal identificado y sus suplentes con la responsabilidad, autoridad y competencia necesarios para desempeñar su rol designado; y

b) procedimientos documentados para guiar sus acciones (véase subcapítulo 8.4.4), incluyendo 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) comunicarse interna y externamente con las partes interesadas relevantes, incluyendo 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 disrupción;

d) facilitar la comunicación estructurada con el equipo de respuesta de emergencias;

e) proporcionar detalles de la respuesta de los medios de comunicación de la organización después de un incidente, incluyendo una estrategia de comunicaciones; y

f) registrar los detalles de la disrupción, las acciones tomadas y las decisiones hechas.

8.4.3.2 Cuando sea aplicable, también se debe considerar e implementar lo siguiente:

a) alertar a las partes interesadas potencialmente afectadas por una disrupción real o inminente; y

b) asegurar una coordinación y comunicación apropiadas entre las múltiples organizaciones que responden.

Los procedimientos de advertencia y comunicación deben ser ejercidos como parte del programa de ejercicios de la organización descrito en el subcapítulo 8.5.

8.4.4 Planes de continuidad del negocio

8.4.4.1 La organización debe documentar y mantener los 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 disrupción y para ayudar a la organización con respuesta y recuperación.

8.4.4.2 Colectivamente, los planes de continuidad del negocio deben contener:

a) detalles de las acciones que tomarán los equipos para:

1) continuar o recuperar las actividades priorizadas dentro de periodos de tiempo predeterminados;

2) monitorear el impacto de la disrupción y la respuesta de la organización a esta;

b) referencia de umbral(es) predefinido(s) y al proceso para activar la respuesta;

c) procedimientos para habilitar la entrega de productos y servicios en la capacidad acordada;

d) detalles para gestionar las consecuencias inmediatas de una disrupción teniendo debidamente en cuenta:

1) el bienestar de las personas;

2) la prevención de futuras pérdidas o falta de disponibilidad de las actividades priorizadas; y

3) el impacto en 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 presentación de informes; y

h) un proceso para suspender operaciones.

Cada plan debe ser utilizable y estar disponible en el momento y lugar en el que sea requerido.

8.4.5 Recuperación

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

8.5 Programa de ejercicios

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

La organización debe conducir 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 metas y objetivos claramente definidos;

c) desarrollen el trabajo en equipo, la competencia, confianza y el conocimiento para aquellos que tienen roles que desempeñar en relación con las disrupciones;

d) en conjunto, a lo largo del tiempo, validen sus estrategias y soluciones de continuidad del negocio;

e) produzcan informes formales posteriores al ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras;

f) se revisen en el contexto de la promoción de la mejora continua; y

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 efectividad de su análisis de impacto en el negocio, evaluación de riesgos, estrategias, soluciones, planes y procedimientos;

b) emprender evaluaciones a través de revisiones, análisis, ejercicios, pruebas, informes posteriores al incidente y evaluaciones de desempeño;

c) conducir evaluaciones de las capacidades de continuidad del negocio de socios y proveedores relevantes;

d) evaluar el cumplimiento de los requisitos legales y regulatorios aplicables, las mejores prácticas de la industria, y la conformidad con su propia política y objetivos de continuidad del negocio; y

e) actualizar la documentación y los procedimientos de manera oportuna.

Estas evaluaciones se deben ser conducidas en intervalos planificados, después de un incidente o activación, y cuando se producen cambios significativos.

9 Evaluación de desempeño

9.1 Monitoreo, medición, análisis y evaluación

La organización debe determinar:

a) que necesita ser monitoreado y medido;

b) los métodos de monitoreo, medición, análisis y evaluación, según sea aplicable, para garantizar la validez de los resultados;

c) cuándo y quién debe realizar el monitoreo y la medición; y

d) cuándo y por quién se deben analizar y evaluar los resultados del monitoreo y la medición.

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

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

9.2 Auditoría interna

9.2.1 Generalidades

La organización debe conducir auditorías internas a intervalos planificados para proporcionar información sobre si el SGCN:

a) es conforme con:

1) los requisitos propios de la organización para su SGCN;

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(s) de auditoría que incluya la frecuencia, los métodos, responsabilidades, requisitos de planificación e informes, que deben tomar en consideración la importancia de los procesos en cuestión y los resultados de auditorías previas;

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

c) seleccionar auditores y conducir auditorías para garantizar la objetividad y la imparcialidad del proceso de auditoría;

d) garantizar que los resultados de las auditorías se informan a los gerentes relevantes;

e) retener información documentada como evidencia de la implementación del programa(s) de auditoria y los resultados de la auditoria;

f) garantizar que cualquier acción correctiva necesaria es tomada sin demora indebida para eliminar las no conformidades detectadas y sus causas; y

g) garantizar que las acciones de seguimiento de auditoría incluyan la verificación de las acciones tomadas y el informe de resultados de la verificación.

9.3 Revisión por la gerencia

9.3.1 Generalidades

La alta dirección debe revisar el SGCN de la organización, a intervalos planificados, para garantizar su continua idoneidad, adecuación y efectividad.

9.3.2 Insumos para la revisión por la gerencia

La revisión por la gerencia debe considerar:

a) el estado de las acciones de revisiones por la gerencia previas;

b) cambios en las cuestiones externas e internas que son relevantes para el SGCN;

c) información sobre el desempeño del SGCN, incluyendo las tendencias en:

1) no conformidades y acciones correctivas;

2) resultados de evaluación del seguimiento y medición;

3) resultados de la auditoría;

d) retroalimentación de las partes interesadas;

e) la necesidad de cambios en el SGCN, incluyendo la política y los objetivos;

f) procedimientos y recursos que podrían usarse en la organización para mejorar el desempeño y efectividad del SGCN;

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 (véase subcapítulo 8.6);

i) riesgos o cuestiones no abordados adecuadamente en cualquier evaluación de riesgos previa;

j) lecciones aprendidas y acciones derivadas de cuasi-accidentes y disrupciones; y

k) oportunidades para la 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 las oportunidades de mejora continua y cualquier necesidad de cambios en el SGCN para mejorar su eficiencia y eficacia, incluyendo lo siguiente:

a) variaciones en el alcance del SGCN;

b) actualización del análisis de impacto en el negocio, evaluación de riesgos, estrategias de continuidad del negocio y soluciones y planes de continuidad del negocio;

c) modificación de procedimientos y controles para responder a cuestiones internas o externas que pueden afectar el SGCN; y

d) cómo se medirá la efectividad de los controles.

9.3.3.2 La organización debe retener información documentada como evidencia de los resultados de la revisión pro la gerencia. Esto debe:

a) comunicar los resultados de la revisión por la gerencia a las partes interesadas relevantes; y

b) tomar las acciones apropiadas en relación con esos resultados.

10 Mejora

10.1 No conformidades y acciones correctivas

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

10.1.2 Cuando ocurre una no conformidad, la organización debe:

a) reaccionar ante la no conformidad y, según sea aplicable:

1) tomar acción para controlarla y corregirla;

2) lidiar con las consecuencias;

b) evaluar la necesidad de actuar para eliminar la(s) causa(s) de la no conformidad, a fin de que esta no sea recurrente u ocurra en otro lugar, mediante:

1) revisión de la no conformidad;

2) determinar las causas de la no conformidad;

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

c) implementar cualquier acción necesaria;

d) revisar la efectividad de cualquier acción correctiva tomada; y

e) hacer cambios en el SGCN, 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 subsecuente tomada; y

b) los resultados de cualquier acción correctiva.

10.2 Mejora continua

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

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

NOTA: La organización puede utilizar los procesos del SGCN, como liderazgo, planificación y evaluación 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