NORMA ISO 22301:2019

ADVERTENCIA

Esta norma **no** forma parte del material del curso. Es sólo para uso interno de NOEDER

Por favor, destruya la misma al finalizar el curso

Contenido

0. INTRODUCCION

0.1 GENERALIDADES

Este documento especifica la estructura y los requisitos para implementar y mantener un Sistema de Gestión de la Continuidad del Negocio (SGCN) que desarrolle la continuidad del negocio que corresponda al importe y tipo de impacto que la organización puede o no asumir después de una interrupción.

Los resultados de mantener un SGCN están determinados por los requisitos legales, reglamentarios, organizativos e industriales 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 urgencia de establecer políticas y objetivos de continuidad del negocio
- Operar y mantener los procesos, la capacidad y los esquemas de respuesta para asegurar que la organización sobreviva a las interrupciones
- Monitorear y revisar el desempeño y la eficacia del SGCN
- El mejoramiento continúo basado en mediciones cualitativas y cuantitativas.

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

- a) Política;
- b) Personal competente con responsabilidades especificas;
- c) Procesos de gestión con relación a:
    - Política;
    - Planificación;
    - Implementación y operación;
    - Evaluación del desempeño;
    - Revisión de la gerencia;
    - Mejoramiento continuo;
- d) Información documentada que soporte el control operativo y permite la evaluación del desempeño.

0.2 BENEFICIOS DEL SISTEMA DE GESTION DE CONTINUIDAD DEL NEGOCIO

El propósito de un SGCN es prepararse para brindar y mantener controles y las capacidades para gestionar el total de la organización para seguir operando durante una interrupción. Para lograr esto, la organización debe:

- a) Desde una perspectiva empresarial:

    - Apoyar sus objetivos estratégicos;
    - Crear una ventaja competitiva;
    - Proteger y mejorar su reputación y credibilidad;
    - Contribuir a la resiliencia organizacional;

- b) Desde una perspectiva financiera:

    - Reducir la exposición legal y financiera;
    - Reducir los costos directos e indirectos de las interrupciones;

- c) Desde la perspectiva de las partes interesadas:

    - Proteger la vida, la propiedad y el medio ambiente;
    - Considerar las expectativas de las partes interesadas;
    - Confiar en las capacidades de la organización para tener éxito;

- d) Desde una perspectiva de procesos internos:

    - Mejorar su capacidad para seguir siendo efectivos durante las interrupciones;
    - Demostrar un control proactivo de los riesgos de manera eficaz y eficiente;
    - Abordar las vulnerabilidades operativas.

0.3 CICLO PLANEAR – HACER- VERIFICAR – ACTUAR (PHVA)

Este documento aplica el ciclo Planear (establecer), Hacer (implementar y operar), Verificar (monitorear y revisar) y Actuar (mantener y mejorar) para implementar, mantener y mejorar de manera continua la eficacia de un SGCN de una organización.

Esto garantiza un nivel de consistencia con otras normas de sistemas de gestión, como ISO 9001, ISO 14001, ISO / IEC 20000-1, ISO / IEC 27001 e ISO 28000, apoyando así la implementación y la operación coherentes e integradas con otros sistemas de gestión relacionados.

De acuerdo con el ciclo PHVA, los Numerales 4 al 10 cubren los siguientes componentes.

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

- El Numeral 5 resume los requisitos específicos del papel de la alta gerencia en el SGCN, y cómo a través de la declaración de las políticas, los líderes comunican claramente sus expectativas a la organización

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

- El Numeral 7 apoya las operaciones de SGCN relacionadas con el establecimiento de las competencias y la comunicación reiterativa según sea necesario con las partes interesadas, al tiempo que se documenta, controla, mantiene y conserva la información documentada requerida.

- El Numeral 8 define las necesidades de continuidad del negocio, determina cómo abordarlas y desarrolla procedimientos para gestionar la organización durante una interrupción.

- El Numeral 9 resume los requisitos necesarios para medir el desempeño de la continuidad del negocio, la conformidad del SGCN con este documento y dirigir la revisión por la dirección.

- El Numeral10 identifica y reacciona ante las no conformidades del SGCN, y el mejoramiento continuo a través de las acciones correctivas.

0.4 CONTENIDO EN ESTE DOCUMENTO

Este documento cumple con los requisitos de ISO para las normas del sistema de gestión. Estos requisitos incluyen una estructura de alto nivel, texto básico idéntico y términos comunes con definiciones esenciales, diseñadas para beneficiar a los usuarios que implementen varias normas de sistema de gestión.

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 pueden ser usados por una organización para implementar un SGCN y evaluar la conformidad. Una organización que desee demostrar su conformidad con este documento puede hacerlo de la siguiente manera:

- Elaborar una autodeterminación o una auto declaración; o
- Solicitar la confirmación de su conformidad por las partes que tengan interés en la organización, como los clientes; o
- Lograr la confirmación de su auto declaración por las partes externas de la organización; o
- Lograr la certificación o registro de su SGCN por una organización externa.

Los numerales del 1 a 3 exponen el alcance, las referencias normativas y los términos y definiciones que se aplican al uso de este documento. Los numerales del 4 a 10 contienen los requisitos que deben utilizarse para evaluar la conformidad de este documento.

En este documento, se usan las siguientes formas verbales:

- "debe" indica un requisito;

- "debería" indica una recomendación;
- "puede" indica en algunas ocasiones un permiso; y en otras, posibilidad o capacidad.

La información marcada como "NOTA" es para la orientación en la compresión o clarificación del requisito asociado. Las “Notas a la entrada” utilizadas en el Numeral 3 proporcionan información adicional que complementa la información terminológica y pueden contener disposiciones relacionadas con el uso de un término.

1. OBJETO Y CAMPO DE APLICACION

Este documento especifica los requisitos para implementar, mantener y mejorar un sistema de gestión para protegerse, reducir la probabilidad de ocurrencia de, prepararse, responder y recuperarse de las interrupciones cuando estas surjan.

Los requisitos que se especifican en este documento son genéricos y están destinados para ser aplicables en todas las organizaciones, o partes de estas, sin tener en cuenta el tipo, tamaño o naturaleza de la organización. El grado de aplicación de estos requisitos depende del ambiente operativo y la complejidad de la organización.

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

- a) Implementen, mantengan y mejoren un SGCN;
- b) Procuren asegurar la conformidad con las políticas de continuidad de negocio establecida;
- c) Tengan la capacidad de continuar entregando sus productos y servicios en una aceptable capacidad predefinida durante una interrupción;
- d) Procuren mejorar su resiliencia a través de la aplicación efectiva del SGCN.

Este documento puede usarse para evaluar la capacidad de la organización para satisfacer sus propias obligaciones y necesidades 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 requisito 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 referenciado (incluidas las enmiendas).

- ISO 22300, Seguridad y resiliencia – Vocabulario

3. TERMINOS Y DEFINICIONES

Para los efectos de este documento, se aplican los términos y definiciones dados en ISO 22300. ISO e IEC mantienen bases de datos terminológicas para su uso en la estandarización en las siguientes direcciones:

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

NOTA: Los términos y definiciones que se mencionan a continuación reemplazan a los que figuran en ISO 22300: 2018.

3.1 ACTIVIDAD (ACTIVITY)

Conjunto de una o más tareas con un resultado definido.

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

3.2 AUDITORIA (AUDIT)

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

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

Nota 2 a la entrada: Una auditoria interna es llevada a cabo por la misma organización (3.21) o una parte externa en su nombre.

Nota 3 a la entrada: Las "Evidencias" y los "criterios" de auditoria se definen en la norma ISO 19011.

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

Nota 5 a la entrada: Una auditoría interna puede usarse para revisión por la dirección y otros fines internos y puede ser la base para la declaración de conformidad de una organización. La independencia se demuestra por la autonomía de la responsabilidad de la actividad (3.1) que se audita. Las auditorías externas incluyen auditorías de segundas y terceras partes. Las auditorías de segundas partes son llevadas a cabo por partes que tienen interés en la organización, tales como clientes, u otras personas en su nombre. Las auditorías de terceras partes se llevan a cabo por organizaciones de auditorías independientes y externas, tales como aquellas que proveen los certificados o registros de conformidad o entes gubernamentales.

Nota 6 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión ISO. Se modificó la definición original adicionando las notas 4 y 5 a la entrada.

3.3 CONTINUIDAD DE NEGOCIO (BUSINESS CONTINUITY)

Capacidad de una organización (3.21) de continuar la oferta de productos y servicios (3.27) dentro de un periodo de tiempo aceptable a una capacidad predefinida durante una interrupción (3.10)

[FUENTE: ISO 22300: 2018, 3.24, modificado – Se reemplazó la definición]

3.4 PLAN DE CONTINUIDAD DE NEGOCIO (BUSINESS CONTINUITY PLAN)

Información documentada (3.11) que orienta a una organización (3.21) para responder a una interrupción (3.10) y reanudar, recuperar y restaurar la oferta de productos y servicios (3.27) de acuerdo con sus objetivos (3.20) de continuidad de negocio (3.3)

[FUENTE: ISO 22300: 2018, 3.26, modificado - Se reemplazó la definición y se eliminó la Nota 1 a la entrada.]

3.5 ANALISIS DEL IMPACTO AL NEGOCIO (BUSINESS IMPACT ANALYSIS BIA)

Proceso (3.26) en el que se analiza el impacto (3.13) de una interrupción (3.10) conforme avanza el tiempo, en la organización (3.21)

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

[FUENTE: ISO 22300: 2018, 3.27, modificado Se reemplazó la definición y se incluyó la Nota 1 a la entrada].

3.6 COMPETENCIA (COMPETENCE)

Habilidad de aplicar los conocimientos y las habilidades para lograr los resultados deseados.

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

3.7 CONFORMIDAD (CONFORMITY)

Cumplimiento de un requisito (3.28)
Nota 1 a la entrada: Este constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sistemas de gestión ISO.

3.8 MEJORAMIENTO CONTINUO (CONTINUAL IMPROVEMENT)

Actividad (3.1) recurrente para mejorar el desempeño (3.23)

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

3.9 ACCION CORRECTIVA (CORRECTIVE ACTION)

Acción para eliminar la causa de una no conformidad (3.19) y prevenir la recurrencia.

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

3.10 INTERRUPCION (DISRUPTION)

Incidente (3.14), bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de productos y servicios (3.27) de acuerdo con los objetivos (3.20) de una organización (3.21)

[FUENTE: ISO 22300: 2018, 3.70, modificado – Se reemplazó la definición]

3.11 INFORMACION DOCUMENTADA (DOCUMENTED INFORMATION)

Información que una organización (3.21) tiene que controlar y mantener, y el medio en el que la contiene.

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

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

- El sistema de gestión (3.16), incluidos los procesos (3.26) relacionados;
- La información generada para que la organización opere (documentación);
- La evidencia de los resultados alcanzados (registros).

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

3.12 EFICACIA (EFFECTIVENESS)

Grado en el cual se realiza las actividades (3.1) planeadas y se logran los resultados esperados

Nota 1 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión ISO.

3.13 IMPACTO (IMPACT)

Resultado de una interrupción (3.10) que afecta los objetivos (3.20)

[FUENTE: ISO 22300: 2018, 3.107, modificado – Se reemplazó la definición]

3.14 INCIDENTE (INCIDENT)

Evento que puede ser, o podría conducir a, una interrupción (3.10), pérdida, emergencia o crisis

[FUENTE: ISO 22300: 2018, 3.111, modificado - Se reemplazó la definición]

3.15 PARTE INTERESADA (INTERESTED PARTY) - (TERMINO

PREFERIDO) ACCIONISTA (STAKEHOLDER) - (TÉRMINO ADMITIDO)

Persona u organización (3.21) que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad (3.1)

Ejemplo: Clientes, propietarios, personal de una organización, proveedores, banca, legisladores, sindicatos, socios o sociedad que pueden incluir competidores o grupos de presión con intereses opuestos.

Nota 1 a la entrada: Una persona encargada puede ser una parte interesada.

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

Nota 3 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sistemas de gestión de ISO. Se modificó la definición original adicionando un ejemplo y las Notas 1 y 2 a la entrada.

3.16 SISTEMA DE GESTION (MANAGEMENT SYSTEM)

Conjunto de elementos de una organización (3.21) interrelacionados o que interactúan para establecer políticas (3.24) objetivos (3.20) y procesos (3.26) para lograr esos objetivos

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

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

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

Nota 4 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión de ISO

3.17 MEDICION (MEASUREMENT)

Proceso (3.26) para determinar un valor

Nota 1 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión ISO.

3.18 MONITOREO (MONITORING)

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 comprobar, supervisar u observar de manera crítica.

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

3.19 NO CONFORMIDAD (NONCONFORMITY)

Incumplimiento de un requisito (3.28)

Nota 1 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión ISO.

3.20 OBJETIVO (OBJECTIVE)

Resultado a lograr.

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

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

Nota 3 a la entrada: Un objetivo puede expresarse de varias maneras. Por ejemplo, como un resultado deseado, como un propósito, como un criterio operativo, como un objetivo de continuidad de negocio (3.3), o mediante el uso de otras palabras similar (por ejemplo, objetivo, meta, propósito).

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

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

3.21 ORGANIZACIÓN (ORGANIZATION)

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridad y relaciones para lograr sus objetivos (3.20)

Nota 1 a la entrada: El concepto de organización incluye, pero no se limita a, un comerciante independiente, una compañía, una corporación, una firma, una empresa, una autoridad, una asociación, una organización benéfica o institución, o parte o combinación de los mismos, bien 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 esenciales de la estructura de alto nivel para los estándares del sistema de gestión ISO. Se modificó la definición original adicionando la Nota a la entrada 2.

3.22 SUBCONTRATAR (OUTSOURCE)

Realizar un acuerdo donde una organización (3.21) externa realiza parte de una función o proceso (3.26) de la organización.

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

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

3.23 DESEMPEÑO (PERFORMANCE)

Resultado medible

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

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

Nota 3 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión de ISO.

3.24 POLITICA (POLICY)

Propósitos y dirección de una organización (3.21), como se expresa formalmente la alta dirección (3.31)

Nota 1 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión de ISO.

3.25 ACTIVDADES PRIORIZADAS (PRIORITIZIED ACTIVITY)

Actividad (3.1) a la que se da urgencia con el fin de evitar impactos (3.13) indeseables para el negocio durante una interrupción (3.10)

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

3.26 PROCESO (PROCESS)

Conjunto de actividades (3.1) interrelacionadas o que interactúan las cuales transforman entradas en salidas

Nota 1 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión de ISO.

3.27 PRODUCTO Y SERVICIO (PRODUCT AND SERVICE)

Salida o resultado que provee una organización (3.21) a las partes interesadas (3.15)

Ejemplo: Productos manufacturados, seguros de automóvil, servicios de enfermería.

[FUENTE: ISO 22300: 2018, 3.181, modificado - El término "productos o servicios" se reemplazó por "productos y servicios" y se reemplazó la definición.]

3.28 REQUERIMIENTOS (REQUIREMENT)

Necesidad o expectativa que se indica, generalmente implícita u obligatoria

Nota 1 a la entrada: “Generalmente implícita” significa que es costumbre o práctica común de la organización (3.21) y de las partes interesadas (3.15) que la necesidad o expectativa en consideración es implícita.

Nota 2 a la entrada: Un requisito específico es aquel que se indica. Por ejemplo, en la información documentada (3.11).

Nota 3 a la entrada: Esto constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel para los estándares del sistema de gestión de ISO.

3.29 RECURSO (RESOURCE)

Todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (ya sea electrónica o no) que una organización (3.21) posee

y que deben tener la disponibilidad para usarse cuando sea necesario, con el fin de operar y lograr su objetivo (3.20)

[FUENTE: ISO 22300: 2018, 3.193, modificado - Se reemplazó la definición.]

3.30 RIESGO (RISK)

Efecto de la incertidumbre en 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: La incertidumbre es el estado, incluso parcial, de la deficiencia en la información relacionada, conocida y comprendida, de un evento, su consecuencia y probabilidad.

Nota 3 a la entrada: El riesgo se caracteriza a menudo por la referencia a posibles "eventos" y "consecuencias" (como se define en la Guía 73 de ISO) de ocurrencia.

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

Nota 5 a la entrada: Este constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sistemas de gestión de ISO. Se modificó la definición adicionando en los "objetivos" para ser consistentes con la NTC ISO 31000.

3.31 ALTA DIRECCION (TOP MANAGEMENT)

Persona o grupo de personas que dirigen y controlan una organización (3.21) en su más alto nivel

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

Nota 2 a la entrada: si el alcance del sistema de gestión (3.16) cubre solo una parte de la 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 esenciales de la estructura de alto nivel de las normas de los sistemas de gestión de ISO.

4. CONTEXTO DE LA ORGANIZACION

4.1 COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO

La organización debe determinar los aspectos externos e internos que sean relevantes para su propósito y que afecten su capacidad para lograr el (los) resultado(s) deseado(s) de su SGCN.

NOTA: Estos aspectos 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 ENTENDIENDO LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

4.2.1 GENERALIDADES

Cuando se establece un SGCN la organización debe determinar:

- a) Las partes interesadas que son relevantes al SGCN
- b) Los requisitos relevantes para esas partes interesadas

4.2.2 REQUISITOS LEGALES Y REGLAMENTARIOS

La organización debe:

- a) Implementar y mantener procesos para identificar, tener acceso y evaluar los requisitos legales y reglamentarios vigentes relacionados con la continuidad de sus productos y servicios, actividades y recursos;
- b) Asegurar de que estos requisitos regulatorios, legales y cualquier otro, vigentes sean tengan en cuenta en la implementación y mantenimiento del SGCN;
- c) Documentar esta información y mantenerla actualizada.

4.3 DETERMINAR EL ALCANCE DEL SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

4.3.1 GENERALIDADES

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

Cuando se determina el alcance, la organización debe considerar:

- a) Las cuestiones externas e internas a los que se hizo referencia en el numeral 4.1;
- b) Los requisitos a los que se hizo referencia en el numeral 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 GESTION DE CONTINUIDAD DE NEGOCIO

La organización debe:

- a) Establecer las partes de la organización que sean incluidas en el SGCN, teniendo en cuenta su locación, tamaño, naturaleza y complejidad;
- b) Identificar productos y servicios que se incluirán en el SGCN.

Cuando se define el alcance del SGCN, la organización debe documentar y aclarar las exclusiones. Estas no deben afectar la responsabilidad y capacidad de la organización para brindar la continuidad de negocio, según lo determinado por el análisis de impacto al negocio o la evaluación del riesgo y los requisitos regulatorios y legales vigentes.

4.4 SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

La organización debe establecer, implementar, mantener y mejorar de manera continua el SGCN, incluyendo 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:

- a) Asegurando que las políticas y los objetivos de continuidad del negocio están establecidos y son compatibles con la dirección estratégica de la organización;
- b) Asegurando la integración de los requisitos de SGCN en los procesos empresariales de la organización;
- c) Asegurando que los recursos necesarios para el SGCN se encuentran disponibles;
- d) Comunicando la importancia de la continuidad del negocio efectiva de acuerdo con los requisitos del SGCN;
- e) Asegurando que el SGCN logre los objetivo(s) deseado(s);
- f) Dirigiendo y apoyando al personal que contribuye a la eficacia del SGCN;
- g) Promoviendo el mejoramiento continuo;
- h) Apoyando otras funciones gerenciales importantes para demostrar liderazgo y compromiso que aplican a sus áreas de responsabilidad.

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

5.2 POLITICA

5.2.1 ESTABLECER LA POLITICA DE CONTINUIDAD DEL NEGOCIO

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

- a) Sea apropiada a los propósitos de la organización;
- b) Proporcione una estructura para establecer los objetivos de continuidad de negocio;
- c) Incluya el compromiso para satisfacer los requisitos aplicables;
- d) Incluya el compromiso de mejoramiento continuo del SGCN.

5.2.2 COMUNICAR LA POLITICA DE CONTINUIDAD DEL NEGOCIO

La política de continuidad del negocio debe:

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

5.3 FUNCIONES, RESPONSABILIDADES Y AUTORIDAD

La alta dirección debe asegurar que la responsabilidad y autoridades para los roles importantes se asignen y se comuniquen al interior de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

- a) Asegurar de que el SGCN cumple con los requisitos de este documento;
- b) Informar acerca del desempeño del SGCN a la alta dirección.

6. PLANIFICACIÓN

6.1 ACCIONES PARA DIRECCIONAR RIESGOS Y LAS OPORTUNIDADES

6.1.1 DETERMINAR LOS RIESGOS Y LAS OPORTUNIDADES

Cuando se realiza la planeación del SGCN, la organización debe considerar las cuestiones a las que se le hace referencia en el Numeral 4.1 y los requisitos contemplados del Numeral 4.2 y determinar los riesgos y oportunidades que deben ser dirigidos a:

- a) Asegurarse que el SGCN pueda lograr el (los) resultado(s) deseado(s);
- b) Prevenir o reducir los resultados indeseados;
- c) Lograr el mejoramiento continuo.

6.1.2 DIRECCIONAR RIESGOS Y OPORTUNIDADES

La organización debe planear:

- a) Acciones para abordar los riesgos y las oportunidades;
- b) Como:
    - 1) Integrar e implementar las acciones en los procesos del SGCN (ver Numeral 8.1);
    - 2) Evaluar la eficacia de estas acciones (ver Numeral 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 abordan en el Numeral 8.2.

6.2 OBJETIVOS PARA LA CONTINUIDAD DE NEGOCIO Y PLANEACION PARA LOGRARLOS

6.2.1 ESTABLECER LOS OBJETIVOS PARA LA CONTINUIDAD DE NEGOCIO

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

Los objetivos para la continuidad de negocio deben:

- a) Ser consistentes con la política de continuidad del negocio;
- b) Ser medible (si es viable);
- c) Tener en cuenta los requisitos vigentes (ver Numerales 4.1 y 4.2);
- d) Ser Monitoreados;
- e) Ser Comunicados;
- f) Estar actualizados según convenga.

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

6.2.2 DETERMINAR LOS OBJETIVOS PARA LA CONTINUIDAD DE NEGOCIO

Al planificar cómo lograr los objetivos para la continuidad de negocio, la organización debe determinar:

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

6.3 PLANEACIÓN DE CAMBIOS EN EL SISTEMA DE GESTION DE CONTINUIDAD DEL NEGOCIO

Cuando la organización determine la necesidad de cambios en el SGCN, incluyendo aquellos identificados en El Numeral10, estos cambios se deben llevar a cabo de manera planificada.

La organización debe considerar:

- a) El propósito del cambio y sus consecuencias potenciales;
- b) La integridad del SGCN;
- c) La disponibilidad de recursos;
- d) La asignación o reasignación de responsabilidades y autoridad.

7 SOPORTE

7.1 RECURSOS

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

7.2 COMPETENCIA

La organización debe:

- a) Determinar las competencias necesarias de la (s) persona (s) que trabajan bajo su propio control y que afecta su desempeño de continuidad de negocio;
- b) Asegurar que estas personas son competentes basándose en la educación, formación o experiencia apropiadas;
- c) Cuando sea aplicable, tomar acciones para adquirir las competencias necesarias y evaluar la eficacia de las acciones tomadas;
- d) Conservar información documentada como evidencia de las competencias.

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

7.3 CONCIENCIACION

Las personas que trabajen bajo el control de la organización deben ser conscientes de:

- a) La política de continuidad del negocio;
- b) Su contribución para la eficacia del SGCN, incluyendo los beneficios de la mejorar del desempeño de la continuidad del negocio;
- c) Las implicaciones de las no conformidades con los requisitos del SGCN;

- d) Sus roles y responsabilidades antes, durante y después de las interrupciones.

7.4 COMUNICACIÓN

La organización debe determinar las comunicaciones internas y externas pertinentes para el SGCN, que incluyan:

- a) Que comunicar;
- b) Cuándo comunicar;
- c) A quién comunicar;
- d) Cómo comunicar;
- e) Quién comunicará.

7.5 INFORMACION DOCUMENTADA

7.5.1 GENERALIDADES

El SGCN de la organización debe incluir:

- a) La información documentada requerida por este documento;
- b) La información documentada determinada por la organización como necesaria 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 el tipo de actividad, procesos, productos y servicios y recursos;
- La complejidad de los procesos y sus interacciones;
- La competencia de las personas.

7.5.2 CREACION Y ACTUALIZACION

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

- a) Identificación y descripción (por ejemplo, un título, fecha, autor o referencia numérica);
- b) Formato (por ejemplo, lenguaje, versión de software, gráficos) y medios (por ejemplo, papel, electrónico);
- c) Revisión y aprobación para conveniencia y adecuación.

7.5.3 CONTROL DE INFORMACIÓN DOCUMENTADA

7.5.3.1 La información documentada que se requiere para el SGCN y por el presente documento debe ser controlará para asegurarse de que:

- a) Que esté disponible y sea idónea para su uso, donde y cuando se necesite;
- b) Que esté protegida adecuadamente (por ejemplo, contra pérdida de confidencialidad, uso inadecuado 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 preservación, incluyendo la preservación de la legibilidad;
- c) Control de cambios (por ejemplo, control de versión);
- d) Conservación y disposición.

La información documentada de origen externo que la organización determina como necesaria para la planificación y operación del SGCN debe identificarse, según sea apropiado, y controlada.

NOTA El acceso puede implicar la decisión de acuerdo con el permiso para ver solamente la información, o el permiso y la autoridad para ver y hacer cambios en la información documentada.

8 OPERACIÓN

8.1 PLANIFICACION Y CONTROL OPERACIONAL

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

- a) El establecimiento los criterios para los procesos;
- b) La implementación del control de 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 llevan a cabo según lo planificado.

La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no intencionados, tomando acciones para mitigar los efectos adversos, si es necesario.

La organización debe asegurar que los procesos subcontratados y la cadena de abastecimiento estén controlados.

8.2 ANÁLISIS DE IMPACTO AL NEGOCIO Y EVALUACION DE RIESGOS

8.2.1 GENERALIDADES

La organización debe:

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

NOTA La organización determina el orden en que se llevan a cabo el análisis de impacto al negocio y la evaluación de riesgos.

8.2.2 ANALISIS DE IMPACTO DEL NEGOCIO (BIA, POR SUS SIGLAS EN INGLES)

La organización debe usar procesos para analizar el impacto en el negocio para determinar los requisitos y prioridades de la continuidad del negocio. El proceso debe:

- a) Definir los tipos de impacto y criterios relevantes en el contexto de la organización;
- b) Identificar las actividades que soportan la provisión de productos y servicios;
- c) Utilizar los tipos de impacto y criterios para evaluar el impacto a lo largo del tiempo que resulten de una interrupción de esas actividades;
- d) Identificar el periodo de tiempo dentro del cual el impacto de no reanudar las actividades sería inaceptable para la organización;

NOTA 1 Esto puede denominarse " el período máximo tolerable de interrupción (MTPD, por sus siglas en inglés)".

- e) Priorizar periodos de tiempo dentro del periodo identificado en el Numeral d) para reanudar las actividades interrumpidas en una capacidad aceptable mínima especificada;

NOTA 2 Este periodo de tiempo puede denominarse " periodo de tiempo objetivo (RTO, por sus siglas en inglés)".

- f) Usar este análisis para identificar actividades prioritarias;
- g) Determinar cuáles son los recursos que se necesitan para soportar las actividades prioritarias;
- h) Determinar las dependencias, incluyendo socios y proveedores, y las interdependencias de las actividades prioritarias.

8.2.3 EVALUACIÓN DE RIESGOS

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

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

La organización debe:

- a) Identificar el riesgo de interrupción de las actividades prioritarias de la organización y de sus recursos requeridos;
- b) Analizar y evaluar los riesgos identificados;
- c) Determinar cuáles riesgos necesitan tratamiento.

NOTA Los riesgos en este subnumeral se relacionan con la interrupción de las actividades de negocio. Los riesgos y las oportunidades relacionados con la eficacia del sistema de gestión se abordan en Numeral 6.1.

8.3 ESTRATEGIAS PARA LA CONTINUIDAD DE NEGOCIO Y SOLUCIONES

8.3.1 GENERALIDADES

Basado en los resultados del análisis de impacto al negocio y evaluación de riesgos, la organización debe identificar y seleccionar las estrategias para la continuidad de negocio que considere opciones para antes, durante y después de una interrupción. Las estrategias para la continuidad de negocio deben componerse de una o más soluciones.

8.3.2 IDENTIFICACIÓN DE ESTRATEGIAS Y SOLUCIONES.

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

- a) Logren los requisitos para continuar y recuperar las actividades prioritarias dentro del periodo de tiempo identificado y la capacidad acordada;
- b) Protejan las actividades priorizadas de la organización;
- c) Reduzcan la probabilidad de interrupción;
- d) Acorten el período de interrupción;
- e) Limiten el impacto de la interrupción en los productos y servicios de la organización;
- f) Proporcionen la disponibilidad adecuada de los recursos.

8.3.3 SELECCIÓN DE ESTRATEGIAS Y SOLUCIONES.

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

- a) Cumplan con los requisitos para continuar y recuperar actividades priorizadas dentro de los plazos identificados y la capacidad acordada;
- b) Consideren el importe y el tipo de riesgo que la organización puede o no asumir;

- c) Consideren los beneficios y costos asociados.

8.3.4 RECURSOS REQUERIDOS

La organización debe determinar los recursos requeridos para implementar las soluciones para la continuidad del negocio seleccionada. Los tipos de recursos a considerar deben incluir, pero no limitarse a:

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

8.3.5 IMPLEMENTACIÓN DE SOLUCIONES

La organización debe implementar y mantener las soluciones para la continuidad de negocio seleccionadas para que puedan activarse cuando sea necesario.

8.4 PLANES Y PROCEDIMIENTOS DE CONTINUIDAD DEL NEGOCIO

8.4.1 GENERALIDADES

La organización debe implementar y mantener esquemas de respuesta que permitan una advertencia oportuna y la comunicación a las partes interesadas relevantes. Debe brindar planes y procedimientos para gestionar la organización durante una interrupción. Los planes y procedimientos deben usarse cuando se requieren activar las soluciones para la continuidad de negocio.

NOTA Hay diferentes tipos de procedimientos que comprenden los planes de continuidad de negocio.

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

Los procedimientos deben:

- a) Ser específicos con respecto a las medidas inmediatos que deben tomarse durante una interrupción;
- b) Ser flexibles para responder a las cambiantes condiciones internas y externas de una interrupción;

- c) Enfocarse en el impacto de los incidentes que potencialmente conduzcan a una interrupción;
- d) Ser efectivos minimizando el impacto a través de la implementación de las soluciones convenientes;
- e) Asignar las funciones y las 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 durante las interrupciones.

8.4.2.2 Los roles y las responsabilidades de cada equipo y las relaciones entre ellos deben establecerse claramente.

8.4.2.3 En conjunto, los equipos deben ser competentes para:

- a) Evaluar la naturaleza y el alcance de una interrupción y su impacto potencial;
- b) Evaluar el impacto contra los limites predefinidos que justifican el inicio de una respuesta formal;
- c) Activar la respuesta conveniente para la continuidad de negocio;
- d) Planificar acciones que necesiten emprenderse;
- e) Establecer prioridades (la primera prioridad debe ser la seguridad de la vida);
- f) Monitorear los efectos de la interrupción y la respuesta de la organización;
- g) Activar las soluciones para la continuidad de negocio;
- h) Comunicarse con las partes interesadas relevantes, las autoridades y los medios.

8.4.2.4 Para cada equipo debe haber:

- a) personal identificado y sus suplentes con las responsabilidades, autoridad y competencias necesarias para desempeñar la función designada;
- b) procedimientos documentados para guiar sus acciones (ver Numeral 8.4.4), incluyendo 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) Comunicar interna y externamente a las partes interesadas relevantes, incluyendo qué, cuándo, con quién y cómo comunicar;

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

- b) Recibir, documentar y responder a las comunicaciones de las partes interesadas, incluyendo cualquier sistema de asesoría nacional o regional o equivalente;
- c) Asegurar la disponibilidad de los medios de comunicación durante una interrupción;
- d) Facilitar la comunicación estructurada con los organismos de socorro;
- e) Brindar detalles de la respuesta a los medios de comunicación de la organización después de un incidente, incluyendo una estrategia de comunicación;
- f) Registrar los detalles de la interrupción, las acciones realizadas y las decisiones tomadas.

8.4.3.2 Donde aplique, debe también considerarse e implementarse lo siguiente:

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

Los procedimientos de comunicación y advertencia deben practicarse como parte del programa de ejercicios de la organización como se describe en el Numeral 8.5.

8.4.4 PLANES PARA LA CONTINUIDAD DE NEGOCIO

8.4.4.1 La organización debe documentar y mantener planes y procedimientos para la continuidad de negocio. Los planes para la continuidad de negocio deben brindar orientación e información para ayudar a los equipos a responder en una interrupción y ayudar a la organización en la respuesta y recuperación.

8.4.4.2 En conjunto, los planes para la continuidad de negocio deben contener:

- a) Detalles de las acciones que los equipos tomarán para:
  - 1) Continuar o recuperar las actividades prioritarias dentro de los periodos de tiempo predeterminados;
  - 2) Monitorear el impacto de la interrupción y la respuesta de la organización hacia ella;
- b) Referencia de los limites predefinidos y los procesos para activar la respuesta;
- c) Procedimientos para permitir la oferta de productos y servicios en una capacidad acordada;
- d) Detalles para gestionar las consecuencias inmediatas de una interrupción teniendo en cuenta:
  - 1) El bienestar de los individuos;
  - 2) La prevención de nuevas pérdidas o la indisponibilidad de las actividades prioritarias;
  - 3) El impacto en el medio ambiente.

8.4.4.3 Cada plan debe incluir:

- a) Propósito, alcance y objetivos;

- b) Funciones y responsabilidades del equipo que implementará el plan;
- c) Acciones para implementar las soluciones;
- d) Información de soporte necesaria para activar (incluyendo los criterios de activación), operar, coordinar y comunicar las acciones de los equipos;
- e) Interdependencias internas y externas;
- f) Los recursos requeridos;
- g) Los reportes requeridos;
- h) Un proceso para retirarlo.

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

8.4.5 RECUPERACIÓN

La organización debe tener procesos documentados para restaurar y volver a las actividades empresariales a partir de las medidas temporales adoptadas durante y después de la interrupción.

8.5 EJERCICIOS Y PRUEBAS

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

La organización debe conducir ejercicios y pruebas que:

- a) Sean consistentes con los objetivos para la continuidad de negocio;
- b) Estén basados en escenarios adecuados que estén bien planificados con objetivos y propósitos claramente definidos;
- c) Desarrollen el trabajo en equipo, competencia, confianza y conocimiento para aquellos que tienen que desempeñar funciones en relación con las interrupciones;
- d) Validen las estrategias y soluciones para la continuidad de negocio a lo largo del tiempo;
- e)Produzcan reportes formalizados después de los ejercicios que contengan resultados, recomendaciones y acciones para implementar mejoras;
- f) Se revisen en el contexto de promoción de mejora continua;
- g) Se desarrollen en intervalos predeterminados y cuando hay cambios significantes dentro de la organización o el contexto en la cual opera.

La organización debe actuar de acuerdo con los resultados de los ejercicios y las pruebas para implementar cambios y mejoras.

8.6 EVALUACIÓN DE LA DOCUMENTACIÓN Y CAPACIDAD DE CONTINUIDAD DE NEGOCIO.

La organización debe:

- a) Evaluar la pertinencia, idoneidad y eficacia del análisis de impacto al negocio, la evaluación de riesgos, estrategias, soluciones, planes y procedimientos;
- b) Realizar evaluaciones a través de revisiones, análisis, ejercicios, reportes, después de incidentes y evaluaciones de desempeño;
- c) Dirigir evaluaciones de la capacidad de continuidad de negocio de los socios y proveedores relevantes;
- d) Evaluar el cumplimiento de los requisitos regulatorios y legales vigentes, buenas prácticas industriales y la conformidad con sus políticas y objetivos de continuidad de negocio;
- e) Actualizar la documentación y los procedimientos de manera periódica.

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

9 EVALUACION DE DESEMPEÑO

9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN.

La organización debe determinar:

- a) Que necesita seguimiento y medición;
- b) Los métodos de seguimiento, medición, análisis y evaluación, necesarios para asegurar resultados válidos;
- c) Cuándo y quién realizará el seguimiento y la medición;
- d) Cuándo y quién realizará el análisis y la evaluación de los resultados del seguimiento y la medición.

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

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

9.2 AUDITORIA INTERNA

9.2.1 GENERALIDADES

La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información de 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 eficazmente.

9.2.2 PROGRAMAS DE AUDITORÍA

La organización debe:

- a) Planear, establecer, implementar y mantener un o varios programas de auditoría, incluya la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la elaboración de informes, que deben tener en consideración la importancia de los procesos involucrados y los resultados de auditorías previas;
- b) Definir los criterios de la auditoría y el alcance de cada auditoría;
- c) Seleccionar los auditores y llevar a cabo auditorías para asegurarse la objetividad y la imparcialidad de los procesos auditados;
- d) Asegurarse de que los resultados de las auditorías se informen a la dirección pertinente;
- e) Conservar información documentada como evidencia de la implementación del programa de auditoría y de los resultados de las auditorías;
- f) Asegurar que las acciones correctivas adecuadas se tomen sin demoras injustificadas para eliminar las no conformidades detectadas y sus causas;
- g) Asegurar que las acciones de auditoría de seguimiento incluyan la verificación de las medidas adoptadas y la presentación de informes de los resultados de verificación.

9.3 REVISIÓN POR LA DIRECCION

9.3.1 GENERALIDADES

La alta dirección debe revisar el SGCN de la organización, en intervalos predeterminados, para asegurar su continua pertinencia, idoneidad y eficacia.

9.3.2 CONSIDERACIONES DE LA REVISIÓN POR LA DIRECCION

La revisión por la dirección debe considerar:

- a) El estado de las acciones de revisiones por la dirección previas;
- b) Cambios de la cuestiones internas y externas que sean relevantes para el SGCN;
- c) Información del desempeño del SGCN, incluyendo tendencias en:
  - 1) No conformidades y acciones correctivas;
  - 2) Seguimiento y resultados de la evaluación de medición;
  - 3) Resultados de auditoría;
- d) Retroalimentación de las partes interesadas;
- e) La necesidad de cambios en el SGCN, incluyendo la política y los objetivos;
- f) Los procedimientos y los recursos que pueden usarse en la organización para mejorar el desempeño y la eficacia del SGCN;
- g) Información del análisis de impacto al negocio y el análisis de riesgos;
- h) Resultados de la evaluación de la documentación y capacidad de continuidad de negocio (ver Numeral 8.6);

- i) Riesgos o asuntos no abordados de manera adecuada en cualquier evaluación de riesgos anterior;
- j) Lecciones aprendidas y acciones derivadas de las cuasi – errores e interrupciones;
- k) Oportunidades para el mejoramiento continuo.

9.3.3 RESULTADOS DE LA REVISIÓN POR LA DIRECCION

9.3.3.1 Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con oportunidades de mejoramiento continuo y cualquier necesidad de cambio en el SGCN para mejorar la eficiencia y eficacia, incluyendo lo siguiente:

- a) Variaciones en el alcance del SGCN;
- 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 los procedimientos y controles para responder a los asuntos internos y externos que puedan impactar el SGCN;
- d) Cómo se medirá la eficacia de los controles.

9.3.3.2 La organización debe conservar información documentada como evidencia de los resultados de la revisión por la dirección. Debe:

- a) Comunicar los resultados de la revisión por la dirección a las partes interesadas relevantes;
- b) Tomar las convenientes acciones relacionadas con esos resultados.

10 MEJORAMIENTO

10.1 NO CONFORMIDAD Y ACCIÓN CORRECTIVA

10.1.1 La organización debe determinar las oportunidades de mejoramiento e implementar las acciones necesarias para lograr los resultados deseados del SGCN.

10.1.2 Cuando ocurra una no conformidad, la organización debe:

- a) Reaccionar ante la no conformidad y cuando sea aplicable:
    - 1) Tomar acciones para controlarla y corregirla;
    - 2) Hacer frente a las consecuencias;
- b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelvan a ocurrir en otra parte, mediante:

- 1) La revisión de la no conformidad;
- 2) La determinación de las causas de la no conformidad;
- 3) La Determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir;

- c) Implementar cualquier acción necesaria;
- d) Revisar la eficacia de cualquier acción correctiva tomada;
- e) Si fuera necesario, hacer los cambios en el SGCN.

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

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

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

10.2 MEJORA CONTINUA

La organización debe mejorar de manera continua la conveniencia, adecuación y eficacia del SGCN, basado en las mediciones cualitativas y cuantitativas.

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

NOTA La organización puede utilizar los procesos del SGCN, como el liderazgo, la planificación y la evaluación del desempeño, para mejorar.

11 BIBLIOGRAFIA

[1] ISO 9001, Sistemas de gestión de calidad – Requisitos

[2] ISO 14001, Sistemas de gestión ambiental. Requisitos con orientación para su uso.

[3] ISO 19011, Directrices para auditar sistemas de gestión

[4] ISO / IEC / TS 17021-6, Evaluación de la conformidad. Requisitos para los organismos que proporcionan auditoría y certificación de sistemas de gestión. Parte 6: Requisitos de competencia para la auditoría y certificación de sistemas de gestión de la continuidad del negocio.

[5] ISO / IEC 20000-1, Tecnología de la información - Gestión del servicio - Parte 1: Requisitos del sistema de gestión del servicio

[6] ISO 22313, Seguridad social - Sistemas de gestión de la continuidad del negocio - Orientación

[7] ISO 22316, Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos

[8] ISO/TS 22317, Seguridad social - Sistemas de gestión de la continuidad del negocio - Directrices para el análisis del impacto del negocio (BIA)

[9] ISO/TS 22318, Seguridad social. Sistemas de gestión de la continuidad del negocio. Directrices para la continuidad de la cadena de suministro.

[10] ISO/TS 22330, Seguridad y resiliencia. Sistemas de gestión de la continuidad del negocio. Directrices para los aspectos de la continuidad del negocio.

[11] ISO/TS 22331, Seguridad y resistencia. Sistemas de gestión de la continuidad del negocio. Directrices para la estrategia de continuidad del negocio.

[12] ISO/IEC 27001, Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos

[13] ISO/IEC 27031, Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la tecnología de la información y la comunicación para la continuidad del negocio

[14] ISO 28000, Especificación para sistemas de gestión de seguridad para la cadena de suministro.

[15] ISO 31000, Gestión de riesgos - Directrices.

[16] IEC 31010, Gestión de riesgos: técnicas de evaluación de riesgos.

[17] Guía ISO 73, Gestión de riesgos - Vocabulario