NORMA TÉCNICA COLOMBIANA NTC – ISO 22301

Seguridad y resiliencia. Sistema de gestión de continuidad de negocio. Requisitos

E:Security and resiliencie. Business continuity managament systems. Requerements

CORRESPONDENCIA: Esta norma es una adopción idéntica (IDT) por traducción de la norma ISO 22301:2019

DESCRIPTORES: continuidad de negocios; sistemas de gestión; resiliencia; seguridad

I.C.S.:03.100.01;03.100.70

CONTENIDO

0. INTRODUCCIÓN

0.1 GENERALIDADES

Este documento especifica la estructura y los requisitos para implementar y mantener un sistema de gestión de continuidad de negocio (SGCN) que desarrolle una continuidad de negocio que corresponda al importe y tipo de impacto que la organizacion puede o no asumir después de una interrupción.

Los resultados de mantener un SGCN están determinados por los requisitos legales, legislativos, organizacionales e industriales, los productos y servicios ofrecidos, los process utilizados, el tamaño y la estructura de la organización, y los requsitos de sus partes interesadas.

Un SGCN enfatiza la importancia de:

- entender las necesidasdes de la organización y la urgencia de establecer políticas y objetivos para la continuidad de negocio;
- operar y mantener los procesos, la capacidad y los esquemas de respuesta para asegurar que la organizacion sobreviva a las interrupciones;
- monitorear y revisar el desempeño y la eficacia del SGCN
- el mejoramiento continuo basado en mediciones cuantitativas y cualitativas.

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:
    1) Política
    2) Planeación;
    3) Implementación y operación;
    4) Evaluación del desempeño;
    5) Revisión por la dirección;
    6) Mejoramiento continuo;

d) Informacion documentada que soporte el control operativo y permita la evaluación del desempeño

0.2 BENEFICIOS DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

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

a) Desde una perspectiva empresarial:

1) Apoyar sus objetivos estratégicos;
2) Crear una ventaja competitiva;
3) Proteger y realizar su reputación y credibilidad
4) Contribuir a la resiliencia organizacional;

b) Desde una perspectiva financiera:

1) Reducir la exposición legal y financiera;
2) Reducir los costos directos e indirectos de las interrupciones;

c) Desde una perspectiva de las partes interesadas;

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

d) Desde una perspectiva de los procesos internos:

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

03 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, tales como, ISO 9001, ISO 14001, 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 del 4 al 10, abarcan los siguientes componentes:

- 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.

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

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

- Numeral 7: apoya las operaciones del 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.

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

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

- Numeral 10: identifica y reacciona antes las no conformidades del SGCN, y el mejoramiento continuo a través de las acciones correctivas.

0.5 CONTENIDO DE ESTE DOCUMENTO

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

Este documento no incluye requisitos especificos 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 para la organización para implementar un SGCN y evaluar la conformidad. Una oraganizacion que desee demostrar su conformidad con este documento, puede hacerlo de la siguiente manera:

- Elaborar una autodeterminación o una auto-declaración ; o

- Lograr la confirmación de su conformidad por las partes que tengan interés en la organización, como 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 al 3 exponen el alcance, las referencias normativas y los términos y definiciones que se aplican al uso de este documento. Los numerales del 4 al 10 contienen los requsitos que deben utilizarse para evaluar la conformidad de este documento.

En este documento, se usan las siguientes formas verbales:

a) “debe“ indica un requisito;
b) “debería“ indica una recomendación;
c) “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“ usadas en el numeral 3 proporcionan información adicional que complementan la información terminológia y pueden contener disposiciones relacionadas con el uso de un término.

SEGURIDAD Y RESILIENCIA.
SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO.REQUISITOS

1 OBJETO Y CAMPO DE APLICACIÓN

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 génericos y están destinados para ser aplicados en todas las organizaciones, o parte 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 organizacines que:

a) Implementen, mantengan y mejoren un SGCN;
b) Procuren asegurar la conformidad con las políticas de continuidad de negocio establecidas;
c) Tengan la capacidad de continuar ofreciendo 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 citan en el texto de tal manera que parte o todo su contenido constituyen requisito de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO 22300, *Security and resilience. Vocabulary*

3 TÉRMINOS Y DEFICINICIONES

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 de ISO: disponible en https://www.iso.org/obp
- Electropiedia IEC: disponible en http://www.electropedia.org/

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

3.1 actividad (activity). Conjunto de una de una o más tareas con un resultado definido.

[FUENTE: ISO 22300:2018, 3.1, modificado- se reemplazó la definición y el ejemplo se elimino]

3.2 auditoría (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 auditoría interna puede ser llevada a cabo por la misma organización (3.21) o por una parte externa en su nombre.

Nota 3 *a la entrada*: Las evidencias y los criterios de auditoría se definen en la norma ISO 19011

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

Nota 5 *a la entrada*: Una auditoría interna puede usarse para la 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 auditorias de segundas y terceras partes. Las auditorias de segundas partes son llevadas a cabo por las partes que tienen intereses de la organización, tales como clientes, u otras personas en su nombre. Las auditorías de terceras partes se llevan a cabo por organizaciones de auditoría independientes y externas, tales como aquellas que proveen los certificados o registros de conformidad o entes gubernamentales.

Nota 6 *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 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 una *interrupción* (3.10) y reanudar, recuperar y restaurar la oferta de *productos y servicios* (3.27) de acuerdo con los objetivos (3.20) de *continuidad de negocio* (3.3).

[Fuente: ISO 22300:2018, 3.26, modificado- se reemplazó la definicion y se eliminó la nota 1 a la entrada]

3.5 análisis de impacto al negocio (business impact análisis, 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 de negocio (3.3).

[Fuente: ISO 23300:2018, 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 consitituye unos de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sitemas de gestión de 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 básicas de la estructura de alto nivel de las normas de los sitemas de gestión de 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 básicas de la estructura de alto nivel de las normas de los sitemas de gestión de ISO.

3.9 acción correctiva (corrective action). Acción para eliminar la causa de una *no conformidad* (3.19) y prevenir su recurrencia.

Nota 1 *a la entrada*: Este constituye uno de los terminos comunes y definiciones básicas de la estructura de alto nivel de las normas de los sitemas de gestión de ISO.

3.10 interrupción (disruption). *Incidente* (3.14), bien sea esperado o no, que causa una alteracion negativa y no planeada de la oferta esperada de los productos y servicios (3.27) de acuerdo con los objetivos (3.20) de la organizacion (3.21).

[Fuente: ISO 22300:2018, 3.70, modificado – se reemplazó la definición].

3.11 información documentada (documented information). Información que una organización (3.21) que tiene que controlar y mantener, y el medio 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 hacer 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 2 *a la entrada*: Este constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sitemas de gestión de ISO.

3.12 eficacia (effectiveness). Grado en el cual se realizan las actividades (3.1) planeadas y se logran los resultados esperados.

Nota 1 a la entrada: este constituye uno de los términos comunes y definiciones esenciales de la estrucutura de alto nivel de las normas de los sistemas de gestión de 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)-término preferido
Accionista (stakeholder)- término admitido

Persona u *organización* (3.21) que puede afectar, verse afectada o percibirse como afectada por una desición 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 persona interesada

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

Nota 3 *a la entrada*: Este constituye uno de los términos comues y definicones esenciales de la estructura de alto nivel de las normas de los sitemas de gestión de ISO. Se modificó la definición original adicionando un ejemplo un ejemplo y las otas a la entrada 1 y 2.

3.16 sistema de gestión (management system). Conjunto de elementos de una *organización* (3.21) interrelacionadas 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, secciones específicas e identificadas de la organización, o una o más funciones dentro de un grupo de organizaciones.

Nota *4 a la entrada*: Este constituye uno de los términos comunes y definiciones esenciles de la estructura de alto de las normas de los sistemas de gestión de ISO.

3.17 medición (measurement). *Proceso* (3.26) para determinar un valor.

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 de ISO.

3.18 monitoreo (monitoring). Determina 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 esencilales de la estrucutura de alto nivel de las normas de los sitemas de gestión de ISO.

3.19 no conformidad (non conformity) Incumplimiento 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 de ISO.

3.20 objetivo (objetive). 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 objetivos financieros, de salud y seguridad, y ambientales) y pueden aplicarse en diferentes niveles (como estratégicos, 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 la palabras similares (por ejemplo, objeto, meta, propósito).

Nota 4 *a la entrada*: En el contexto de los *sitemas de gestión* (3.16) de continuidad de negocio, la *organización* (3. 21) establece los objetivos de continuidad de negocio, de acuerdo con las politicas (3.24) de la continuidad de negocio, de acuerdo con las *políticas* (3. 24) de continuidad de negocio para lograr los resultados específicos.

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.

3.21 organización (organization). Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridad y relaciones para lograr su *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 combinación de los mismos, bien sea incorporadao no, pública o privada

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

Nota 3 *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 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 esta 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 contituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sistemas de gestión de ISO.

3.23 desempeño (performance). Resultado medible.

Nota 1 *a la entrada*: el desempeño puede ser relacionado con hallazagos cuantitativos o cualitativos.

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

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

3.24 política (policy). Propósitos y dirección de una organización (3.21) como expresa formalmente la alta dirección (3.21)

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 de ISO.

3.25 actividad priorizada (prioritized activity). Actividad (3.1) a la que se le da urgencia con el fin de evitar *impactos* (3.13) indeseables para el negocio durante una interrupción (3.10).

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

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 sitemas de gestión de ISO.

3.27 Productos y servicios (product and service). Salida o resultado que provee una gran *organización* (3.21) a las *partes interesadas* (3.15)

Ejemplo Productos manufacturados, seguro de automóvil, servicios de enfermería.

[Fuente ISO 22300; 2018, 3.181, El término ´´ productos o servicios´´ y se reemplazó por ´´ productos y servicios´´ y se reemplazó la definición

3.28 requisito (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 consideracion 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*: este constituye uno de los términos comunes y definiciones esenciales de la estrucuta de alto nivel de las normas de los sitemas de gestión de ISO.

3.29 recuros (resource). Todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (bien sea electrónica o no) que una *organización* (3.21) posee y que tienen que tener disponibilidad para usarse cuando sea necesario, con el fin de operar y lograr su *objetivo* (3.20).

[Fuente ISO 22300: 2018, 3.103, modificado- se reemplazó la definición].

3.30 riesgo (risk). Efecto de la incertidumbre den los o*bjetivos* (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 guia 73 de ISO) o la combinación de ambos.

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 dirreción (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 de un *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:* Este constituye uno de los términos comunes y definiciones esenciales de la estructura de alto nivel de las normas de los sitemas de gestión de ISO.

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 COMPRENDER 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 el (los) resultado(s) deseado(s) de su SGCN

Nota Estas cuestiones se verán influenciados por los objetivos generales de la organización, sus productos y servicios y el importe y tipo de riesgo que pueda o no asumir.

4.2 COMPRENDER 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 para el 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 tenidos en cuenta en la implementación y mantenimiento del SGCN;

c) documentar eta 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 hizo referencia en el numero 4.1;
b) Los requisitos a los que 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 de sistema de gestión de continuidad de negocio

La organización debe:

a) establecer las partes de la organización que serán incluidas en el SGCN, teniendo en cuenta su locación, tamaño, naturaleza y complejidad;

b) identificar los productos y servicios que se incluirán en el SGCN.

4.4 SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO

La organización de establecer, implementar, mantener y mejorar de manera continua el SGCN incluyendo los procesos necesarios y sus interrelaciones, de acuerdo con los requisitos de este documento.

5 LIDERAZGO

5.1 LIDERAZGO Y COMPROMISO

La alta direccion debe demostrar liderazgo y comprzomiso con respecto al SGCN de la siguiente forma:

a) Asegurando que las políticas y los objetivos de continuidad de negocio están establecidos y son compatibles con la dirección estratégica de la organización;

b) Asegurando la integración a los requisitos del SGCN en los procesos empresariales de la organización;

c) Asegurando que los recursos necesarios para el SGCN se encuentren disponibles

d) Comunicando la importancia de la continuidad de negocio efectiva de acuerdo con los requisitos del SGCN;

e) Asegurando que el SGCN logre el (los) objetivo(s) deseado(s);

f) Dirigiendo y apoyando el 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 a 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 POLÍTICAS

5.2.1 Establecer la política de continuidad de negocio

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

a) Sea apropiada a los propósitos de la organizacón;
b) Proporcione una estructura para establecer los objetivos de continudad
c) Incluya el compromiso para satisfacer los requisitos vigentes;
d) Incluya el compromiso para el mejoramiento continuo del SGCN.

5.2.2 Comunicar la política de continuidad de negocio

La política de continuidad de negocio debe:

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

5.2.3 Funciones, responsabilidades y autoridad

La alta dirección debe asegurarse de que la responsabilidad y la autoridad para los roles importantes se asignen y comuniquen dentro de la organización.

La alta direccion 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 PLANEACIÓN

6.1 ACCIONES PARA ABORDAR LOS RIESGOS Y LAS OPORTUNIDADES

6.1.1 Determinar los riesgos y las oportunidades

Al realizar la planeación del SGCN, la organización debe considerar las cuestiones a las que se hace referencia en el numeral 4.1 y los requisitos del numeral 4.2 y determinar los riesgos y las oportunidades que necesitan abordarse para:

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 Abordar 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)

6.2 OBJETIVOS PARA LA CONTINUIDAD DE NEGOCIO Y LA PLANEACIÓN 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 de negocio;

b) ser medibles (si es viable);

c) Tener en cuenta los requisitos vigentes (ver numerales 4.1 y 4.2);

d) Monitorearse;

e) Comunicarse;

f) Actualizarse según convenga.

g) Actualizarse 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 rerecursos 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 GESTIÓN DE CONTINUIDAD DE NEGOCIO

Cuando la organización determine la necesidad de cambios en el SGCN, incluyendo aquellos identificados en el numeral 10, 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 con el SGCN;
c) La disponibilidad de recursos;
d) La asignación o reasignación de responsabilidad 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 las personas 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 ejempo la formación, de tutoria, o la reasignación de personas empleadas actualmente; o a la contratación de personas empleadas actualmente; o la contratación de personas competentes

7.3 CONOCIMIENTO

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

a) La política de continuidad de negocio;

b) Su contribución para la eficacia del SGCN, incluyendo los beneficios de mejorar el desempeño de la continuidad de negocio;

c) Las implicaciones de las no conformidades con los requisitos del SGCN;

d) Sus funciones 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) Qué comunicar;

b) Cuándo comunicar;

c) A quién comunicar;

d) Cómo comunicar;*22301*

e) Quién comunicará.

7.5 INFORMACIÓN DOCUMENTADA

7.5.1 Generalidades

El SGCN de la organización debe incluir:

a) La información documentada requerida por este documento;

b) La información documentada que la organización determina como necesaria para la eficacia del SGCN.

Nota la extensión 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 sus procesos y sus interrelaciones;

- La competencia de las personas.

7.5.2 Creación y actualización

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

a) Identificación y descripción (por ejemplo, título, fecha, autor o referencia numérica);

b) Formato (por ejemplo, lenguaje, versión del software, gráfico) y medios de soporte (por ejemplo, papel, electrónico);

c) Revisión y aprobación para convivencia y adecuación.

7.5.3 Control de la formación documentada

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

a) que esté disponible y sea idónea para su uso, cuando y donde se necesite;

b) Que esté protegida adecuadamente (por ejemplo, de 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 preservación de 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 controlar.

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 PLANIFICACIÓN Y CONTROL OPERACIONAL

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

a) El establecimiento de 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 abastacimiento sean controlados.

8.2 ANÁLISIS DE IMPACTO AL NEGOCIO Y EVALUACIÓN DE RIESGOS

8.2.1 Generalidades

La organización debe:

a) Implementar y mantener procesos y sistemáticos para analizar el impacto empresarial y evaluar los riesgos de interrupción;

b) Revisar el análisis de impacto al negocio y la evaluación de riesgos en intervalos planificados y cuando haya cambios significativos y cuando haya cambios significativos dentro de la organización o en el contexto en el cual opera.

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

8.2.2 Análisis de impacto al negocio (BIA, por sus siglas en inglés)

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

a) Definir los tipos de impacto y criterios relevantes para el contexto de la organización;

b) Identificar las actividades que soportan la provisión de productos y servicios;

c) Usar 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 se puede denominarse el periodo máximo tolerable de interrupción, MTPD, por sus siglas en inglés.

e) Priorizar períodos 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 siglas en inglés.

f) Usar este análisis para identificar actividades prioritarias

g) Determinar cuáles recursos 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 evalación de riesgos

Nota el proceso para la elaboración de riesgos se aborda en la norma ISO 31000

La organización debe :

a) Indetificar 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 el numeral 6.1

8.3 ESTRATEGIAS PARA LA CONTINUIDAD DE NEGOCIO Y SOLUCIONES

8.3.1 Generalidades

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

8.3.2 identificación de estrategias y soluciones

La identificación de las estrategias y soluciones debe basarse en la medida que estas.

a) Logren los requisitos para continuar y recuperar las actividades prioritarias dentro del periodo de tiempo identificado y la capacidad acordada,

b) Consideren el importe y tipo de riesgo que la organización puede o no asumir;

c) Consideren los costos y los beneficios asociados.

8.3.3 Selección de estrategias y soluciones

La selección debe basarse en la medida que las estrategías y soluciones:

a) Cumpla con los requisitos para continuar y recuperar las actividades prioritarias dentro del período de tiempo identificado y a la capacidad acordada;

b) Considere el importe y tipo de riesgo que la organización puede o no asumir;

c) Considere los beneficios y costos asociados

8.3.4 Requisitos de recursos

La organización debe determinar los requisitos de los recursos para implementar las soluciones para la continuidad de 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 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 PARA LA CONTINUIDAD DE 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 comprendanlos planes para la 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 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 ello

8.4.2 Esquemas de respuesta

8.4.2.1 La organización debe implementar y mantener un esquema, identificado con uno o más equipos responsables, para responder las interrupciones

8.4.2.2 Las funciones 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 límites 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) 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 internas y externamente a las partes interesadas relevantes, incluyendo qué, cuándo, con quién y qué comunicar;

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

b) Recibir, comunicar y responder a las comunicaciones de las partes interesadas, incluyendo cualquier sistema de asesoría nacional o regional o su equivalente;

c) Asegurar la disponibilidad de los medios de comunicación durante la 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 Cuando sea necesario, debe 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) detalle 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 imapcto de la interrupción y la respuesta de la organización hacia ella;

c) Referencia de los límites predefinidios y los procesos para activar la respuesta;

d) 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 disponibilidad 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) Requisitos de los recursos;

g) Requisitos para los reportes;

h) Un proceso para darse de baja.

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 PROGRAMA DE EJERCICIOS

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 estrategías 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 desarrollan intervalos predeterminados y cuando hay cambios significantes dentro de la organización o el contexto en el 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 DE CONTINUDIAD DE NEGOCIO

La organización debe:

a) Evaluar la pertinencia, idoneidad y eficacia del análisis de impacto al negocio, la evaluación del riesgo, estrategias, soluciones, planes y procedimientos;

b) Realizar evaluaciones a través de revisiones, análisis, ejercicios, pruebas, reportes después de incidentes y evaluaciones del desempeño;

c) Dirigir evaluaciones de la capacidad de continuidad de negocio de los socios y proovedores 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 realizarse en intervalos predeterminados, después de un incidente o activación y cuando se presenten cambios significativos.

9 EVALUACIÓN DEL DESEMPEÑO

9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La organización debe determinar:

a) qué necesita seguimiento y medición;

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

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

c) 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 AUDITORÍA INTERNA

9.2.1 Generalidades

La organización debe llevar a cabo auditarías 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 se mantiene eficazmente.

9.2.2 Programa(s) de auditoria

La organización debe:

a) planear, establecer, implementar y mantener uno o varios programas de auditoria 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 las auditorias previas;

b) definir los criterios de la auditoria y el alcance de cada auditoria;

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 auditoria y de los resultados de las auditorías;

f) asegurar que las acciones correctivas adecuadas se tomen sín demoras injustificadas para eliminar las na conformidades detectadas y sus causas;

g) asegurar que las acciones de auditorías de seguimiento incluyan la verificación de las medidas adoptadas y la presentación de informes de los resultados de verificación.

9.3 REVISIÓN POR LA DIRECCIÓN

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 dirección

La revisión por la dirección debe considerar:

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

b) cambios de las cuestiones internas y externas que sean relevantes para el SGCN;

c) Información del desempeño del SGCN, incluyendo tendecias en;

   1) No conformidades y acciones correctivas;
   2) Seguimiento y resultados de la evaluación de medición;
   3) Resultados de auditoria;

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 negocio (ver numeral 8.6);

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 dirección

9.3.3.1 Los resultados de la revisión por la dirección deben incluir decisiones relacionadas con las 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 para la 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) como se medirá la eficacia de los controles.

9.3.3.2 La organización debe conservar la información documentada como evidencua 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 confomidad , 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 otro parte, mediante:

1) La revisión de la no conformidad;
2) La determinación de las causas de la no conformidad;
3) la determinación de sí 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 CONTINUO

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 análisíis y la evaluación, y los resultados de la revisión de la dirección, para determinar sí hay necesidades u oportunidades, relacionadas con la empresa, o el SGCN, que considerarse parte de la mejora continua.

Nota La organización puede usar los procesos del SGCN, como el liderazgo, la planeación y la evaluación del desempeño para mejorar.

11 BIBLIOGRAFIA

[1] ISO 9001, Quality management systems. Requirements

[2] ISO 14001, Enviranmental 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 Sator. Service management. Part 1: Service management
system requirements

ISO 28000, Specification for security management systems for the supply chain

ISO 31000, Risk management. Guidelines

IEC 31010, Risk management. Risk assessment techniques

ISO Guide 73, Risk management. Vocabulary