Sustento del uso justo de Materiales Protegidos

derechos de autor para fines educativos

UCI
Universidad para la Cooperación Internacional

UCI
Sustento del uso justo de materiales protegidos por
derechos de autor para fines educativos

El siguiente material ha sido reproducido, con fines estrictamente didácticos e ilustrativos de los temas en cuestión, se utilizan en el campus virtual de la Universidad para la Cooperación Internacional – UCI – para ser usados exclusivamente para la función docente y el estudio privado de los estudiantes pertenecientes a los programas académicos.

La UCI desea dejar constancia de su estricto respeto a las legislaciones relacionadas con la propiedad intelectual. Todo material digital disponible para un curso y sus estudiantes tiene fines educativos y de investigación. No media en el uso de estos materiales fines de lucro, se entiende como casos especiales para fines educativos a distancia y en lugares donde no atenta contra la normal explotación de la obra y no afecta los intereses legítimos de ningún actor.

La UCI hace un USO JUSTO del material, sustentado en las excepciones a las leyes de derechos de autor establecidas en las siguientes normativas:

a- Legislación costarricense: Ley sobre Derechos de Autor y Derechos Conexos, No.6683 de 14 de octubre de 1982 - artículo 73, la Ley sobre Procedimientos de Observancia de los Derechos de Propiedad Intelectual, No. 8039 – artículo 58, permiten el copiado parcial de obras para la ilustración educativa.
b- Legislación Mexicana; Ley Federal de Derechos de Autor; artículo 147.
c- Legislación de Estados Unidos de América: En referencia al uso justo, menciona: "está consagrado en el artículo 106 de la ley de derecho de autor de los Estados Unidos (U.S,Copyright - Act) y establece un uso libre y gratuito de las obras para fines de crítica, comentarios y noticias, reportajes y docencia (lo que incluye la realización de copias para su uso en clase)."
d- Legislación Canadiense: Ley de derechos de autor C-11– Referidos a Excepciones para Educación a Distancia.
e- OMPI: En el marco de la legislación internacional, según la Organización Mundial de Propiedad Intelectual lo previsto por los tratados internacionales sobre esta materia. El artículo 10(2) del Convenio de Berna, permite a los países miembros establecer limitaciones o excepciones respecto a la posibilidad de utilizar lícitamente las obras literarias o artísticas a título de ilustración de la enseñanza, por medio de publicaciones, emisiones de radio o grabaciones sonoras o visuales.

Además y por indicación de la UCI, los estudiantes del campus virtual tienen el deber de cumplir con lo que establezca la legislación correspondiente en materia de derechos de autor, en su país de residencia.

Finalmente, reiteramos que en UCI no lucramos con las obras de terceros, somos estrictos con respecto al plagio, y no restringimos de ninguna manera el que nuestros estudiantes, académicos e investigadores accedan comercialmente o adquieran los documentos disponibles en el mercado editorial, sea directamente los documentos, o por medio de bases de datos científicas, pagando ellos mismos los costos asociados a dichos accesos.

G

Gestión y Calidad

INTE ISO 22301:2015

Seguridad de la sociedad. Sistemas de gestión de continuidad del negocio.

Requisitos.

Correspondencia: Esta norma nacional es idéntica a la norma internacional ISO 22301:2012, " Societal security — Business continuity management systems — Requirements".

Miembros de

Fecha: 2015-03-10
Primera Edición
Secretaría: INTECO
Editada e impresa por ©INTECO

ICS 03.100.01

CONTENIDO PÁGINA

PRÓLOGO

El Instituto de Normas Técnicas de Costa Rica, INTECO, es el organismo nacional de normalización, según la Ley 8279 de 2002.

El INTECO es una entidad de carácter privado, sin ánimo de lucro, cuya Misión es fundamental para brindar soporte y desarrollo al productor y protección al consumidor. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el periodo de Consulta Pública, este último caracterizado por la participación del público en general.

Esta norma INTE/ISO 22301:2015 fue aprobada por la Comisión Nacional de Normalización de INTECO en la fecha del 2015-03-10.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación se mencionan las empresas que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico.

MIEMBRO	ORGANIZACIÓN
Johnny Vásquez **(Presidente)**	TENSTEP
Harold Cordero	ICE
Diego Cardoza Cinthya Alpizar	NAP
Franklin Giralt Amador Ricardo Morales	BCCR
Víctor Zúñiga	Ti Solutions
Rodolfo Romero Álvaro Montero	UCR
Mauricio Solano	Banco Lafise
Mauren Muñoz	BAC Credomatic
Karol Cordero	PWC
Roger Forbes Gabriela Román	CEGESTI
Manuel Antonio Arias	Dos Pinos
Randall Villalobos	Banco Nacional

0 INTRODUCCIÓN

0.1 Generalidades

Esta norma específica los requisitos para la creación y gestión de un Sistema de Gestión de Continuidad del Negocio (SGCN) efectivo.

Un SGCN hace énfasis en la importancia de:

- Entender las necesidades de la organización y la necesidad de establecer la política y objetivos de Continuidad del Negocio.
- Implementar y operar los controles y medidas para administrar la capacidad general de una organización para responder a incidentes disruptivos.
- Dar seguimiento y revisar el desempeño y eficacia del SGCN; y
- Mejorar continuamente basado en mediciones objetivas.

El SGCN, como todos los sistemas de gestión, contiene los siguientes componentes claves:

a) Una política;
b) Personas con responsabilidades definidas;
c) Gestión de los procesos relativos a:
    1) Política,
    2) Planeamiento,
    3) Implementación y operación,
    4) Evaluación de desempeño,
    5) Análisis de la gestión, y
    6) Mejoramiento.
d) Documentación que proporcione evidencia auditable; y
e) Cualquier proceso de gestión de la continuidad del negocio pertinente para la organización.

La continuidad del negocio contribuye a una sociedad con mayor resiliencia. La comunidad en general, el impacto del ambiente en la organización, así como otras organizaciones deben considerarse en el proceso de recuperación.

0.2 El modelo PLANEAR- HACER- VERIFICAR- ACTUAR (PHVA)

Esta norma aplica el modelo "Planear-Hacer-Verificar-Actuar" (PHVA) para planear, establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar continuamente la eficacia de un SGCN en la organización.

Esto asegura un cierto grado de coherencia con otras normas de sistemas de gestión, tales como la norma INTE/ISO 9001 Sistema de Gestión de Calidad, INTE/ISO 14001, Sistema de Gestión Ambiental, INTE/ISO/IEC 27001 Sistema de Gestión en Seguridad de la Información, ISO/IEC20000-1 Gestión de servicios, y la norma INTE/ISO 28000 Sistema de Gestión de Seguridad para la Cadena de Suministro, apoyando de este modo la implementación coherente e integrada y la operación de con los sistemas de gestión relacionados.

La Figura 1 ilustra cómo un SGCN toma como entradas las partes interesadas y los requisitos para la gestión de la continuidad y a través de las acciones y procesos necesarios, produce resultados de la continuidad del negocio (por ejemplo: gestión de continuidad del negocio) que cumplen con esos requisitos.

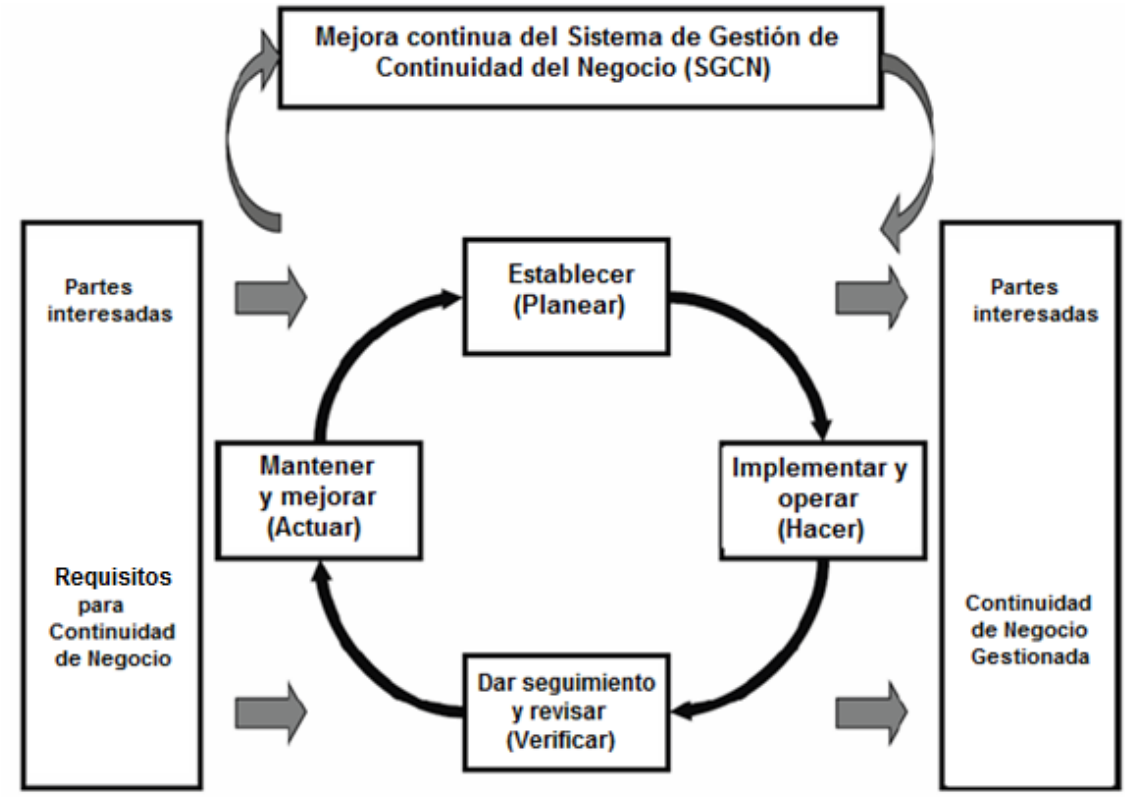

Figura 1. Ciclo PHVA aplicado a los procesos de SGCN

Tabla 1. Explicación del modelo de PHVA

Plan (Establecer)	Establecer la política, objetivos, metas, controles, procesos y procedimientos de continuidad del negocio pertinentes para mejorar la continuidad del negocio, con el fin, de entregar resultados que se alineen con todos los objetivos y políticas de la organización.
Hacer (Implementar y operar)	Implementar y operar la política, controles, procesos y procedimientos de continuidad del negocio.
Verificar (Dar seguimiento y revisar)	Dar seguimiento y revisar el desempeño contra la política y los objetivos de continuidad del negocio, reportar los resultados a la Dirección para la revisión, y determinar y autorizar las acciones para la solución y mejora.
Actuar (Mantener y mejorar)	Mantener y mejorar el SGCN tomando acción correctiva, basada en los resultados de la revisión por la Dirección y la revalorización del alcance del SGCN y la política y los objetivos de continuidad del negocio.

0.3 Componentes del PHVA en esta norma

En esta norma internacional, en los capítulos del 4 al 10, del modelo PHVA como se muestra en la Tabla 1, se cubren los siguientes componentes:

- El capítulo 4 es un componente de Planear. Introduce los requisitos necesarios para establecer el contexto del SGCN que se aplica a la organización, así como las necesidades, requisitos y alcance.

- El capítulo 5 es un componente de Planear. Resume los requisitos específicos para el papel de la alta dirección en el liderazgo del SGCN, y cómo articula sus expectativas a la organización a través de la declaración de la política.

- El capítulo 6 es un componente de Planear. Describe los requisitos, así como lo que se refiere al establecimiento de objetivos estratégicos y los principios que rigen el SGCN en su conjunto. El contenido del capítulo 6 difiere del establecimiento de oportunidades de tratamiento del riesgo derivadas de la valoración del riesgo, así como del análisis de impacto en el negocio (BIA, por sus siglas en inglés) derivado de los objetivos de recuperación.

NOTA Los requisitos para el análisis de impacto en el negocio y el proceso de valoración del riesgo se detallan en el capítulo 8.

- El capítulo 7 es un componente de Planear. Soporta las operaciones del SGCN relacionadas con establecer la competencia y la comunicación sobre una base recurrente o según se requiera, con las partes interesadas, al mismo tiempo documentar, controlar, mantener y conservar la documentación requerida.

- El capítulo 8 es un componente de Hacer. Define los requisitos de continuidad del negocio, determina la forma de abordarlos y desarrolla los procedimientos para gestionar un incidente disruptivo.

- El capítulo 9 es un componente de Verificar. Resume los requisitos necesarios para medir el desempeño de la continuidad del negocio, el cumplimiento del SGCN con la norma, las expectativas de la administración y busca retroalimentar a la administración respecto a sus expectativas.

- El capítulo 10 es un componente de Actuar. Identifica y actúa sobre las no conformidades del SGCN a través de una acción correctiva.

Seguridad de la sociedad. Sistemas de gestión de continuidad del negocio. Requisitos.

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma internacional para la gestión de continuidad del negocio especifica los requisitos para planificar, establecer, implementar, operar, dar seguimiento, revisar, mantener y mejorar continuamente un sistema de gestión documentado para protegerse, reducir la posibilidad de ocurrencia, prepararse, responder y recuperarse de los incidentes disruptivos cuando ocurran.

Los requisitos especificados en esta norma internacional son genéricos y se pretende que sean aplicables a todas las organizaciones o partes de estas, independiente del tipo, tamaño y naturaleza de la organización. El grado de aplicación de estos requisitos depende del entorno operativo de la organización y su complejidad.

No es la intención de esta norma internacional proporcionar uniformidad en la estructura de un SGCN, sino para que una organización diseñe un SGCN que sea apropiado para sus necesidades y que cumpla con los requisitos de sus partes interesadas, estas necesidades están determinadas por los requisitos legales, reglamentarios, organizacionales, y de la industria, los productos y servicios, los procesos empleados, el tamaño y la estructura de la organización y los requisitos de sus partes interesadas.

Esta norma internacional es aplicable a todos los tipos y tamaños de las organizaciones que desean:

a) Establecer, implementar, mantener y mejorar un SGCN

b) Garantizar la conformidad con la política establecida de la continuidad del negocio.

c) Demostrar la conformidad a otros.

d) Buscar la certificación/registro de su SGCN por un organismo acreditado de certificación de tercera parte, o

e) Hacer una auto-determinación y auto-declaración de conformidad con esta norma.

Esta norma internacional puede ser utilizada para evaluar la capacidad de una organización de satisfacer sus propias necesidades de continuidad y obligaciones.

2 NORMAS DE REFERENCIA

No se citan normas para consulta. Este apartado se incluye con el propósito de mantener un orden numérico de los capítulos similar al de otras normas.

3 TÉRMINOS Y DEFINICIONES

Para el propósito de este documento, los siguientes términos y definiciones aplican:

3.1 actividad

procesos o conjunto de procesos realizados por una organización (o en su nombre) que produce o apoya uno o más productos y servicios.

EJEMPLO Los procesos de cuentas, *Call Center*, TI, fabricación, distribución.

3.2 auditoría

proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla de manera objetiva con el fin determinar el grado en que los criterios de la auditoría se cumplen.

NOTA 1 Una auditoría puede ser una auditoría interna (primera parte) o una auditoría externa (segunda o tercera parte), y puede ser una de auditoría combinada (combinación de dos o más disciplinas).

NOTA 2 "La evidencia de auditoría" y "criterios de auditoría" se definen en la norma INTE/ISO 19011.

3.3 continuidad del negocio

Capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posterior a un incidente disruptivo.

[Fuente: INTE/ISO 22300]

3.4 gestión de la Continuidad del negocio

proceso integral de gestión que identifica las amenazas potenciales para una organización y los posibles impactos para las operaciones del negocio de estas amenazas, en caso de que ocurran y proporciona un marco para la construcción de la resiliencia de la organización con la capacidad de una respuesta efectiva que salvaguarde los intereses de sus partes interesadas clave, así como su reputación, marca y actividades que crean valor.

3.5 sistema de gestión de continuidad del negocio SGCN

parte del sistema general de gestión que establece, implementa, opera, da seguimiento, revisa, mantiene y mejora la continuidad del negocio .

NOTA El sistema de gestión incluye la estructura organizativa, las políticas, actividades de planificación, responsabilidades, procedimientos, procesos y recursos.

3.6 plan de continuidad del negocio

procedimientos documentados que guían a las organizaciones para responder, recuperar, reanudar y restaurar a un nivel pre-definido de operación después de una interrupción.

NOTA Típicamente, esto incluye los recursos, servicios y actividades necesarios para asegurar la continuidad de las funciones críticas del negocio.

3.7 programa de continuidad del negocio

proceso continuo de gestión y gobernanza apoyado por la alta dirección y los recursos adecuados para implementar y mantener la gestión de la continuidad del negocio .

3.8 análisis de impacto en el negocio
proceso del análisis de actividades y el efecto que la interrupción del negocio podría tener sobre ellas.

[Fuente: INTE/ISO 22300]

3.9 competencia
capacidad de aplicar conocimientos y habilidades para alcanzar los resultados previstos.

3.10 conformidad
cumplimiento de un requisito

[Fuente: INTE/ISO 22300]

3.11 mejora continua

actividad recurrente para mejorar el desempeño

[Fuente: INTE/ISO 22300]

3.12 corrección
acción para eliminar una no conformidad detectada

[Fuente: INTE/ISO 22300]

3.13 acción correctiva
acción para eliminar la causa de una no conformidad y para evitar que vuelva a ocurrir.

NOTA En el caso de resultados no deseados, son necesarias acciones para minimizar o eliminar las causas y reducir su impacto, prevenir que vuelvan a ocurrir. Estas acciones se encuentran fuera del concepto de "acción correctiva" en el sentido de esta definición.

[Fuente: INTE/ISO 22300]

3.14 documento
información y su medio de soporte.

NOTA 1 El medio puede ser papel, disco magnético, óptico o electrónico, fotografía o muestra maestra, o una combinación de estos.

NOTA 2 Un conjunto de documentos, por ejemplo especificaciones y registros, se denominan "documentación".

3.15 información documentada
información requerida para ser controlada y mantenida por una organización y el medio en el que está contenido.

NOTA 1 Información documentada puede ser en cualquier formato y los medios de comunicación de cualquier fuente.

NOTA 2 La información documentada se puede referir a.
- El sistema de gestión, incluyendo los procesos relacionados;
- La información creada por la organización con el fin de operar (la documentación);
- La evidencia de los resultados obtenidos (registros).

3.16 eficacia
grado en el cual se realiza las actividades planificadas y se logran los resultados planificados

[Fuente: INTE/ISO 22300]

3.17 evento

ocurrencia o cambio de un conjunto particular de circunstancias

NOTA 1 Un evento puede ser único o repetirse, y puede tener varias causas.

NOTA 2 Un evento puede consistir en algo que no se llega a producir.

NOTA 3 Algunas veces, un evento se puede calificar como un "incidente" o un "accidente".".

NOTA 4 Un evento sin consecuencias (3.6.1.3) también se puede citar como "cuasi accidente", o "incidente".

[FUENTE: Guía INTE/ISO 73]

3.18 ejercicio

proceso de entrenamiento para evaluar, practicar y mejorar el desempeño en una organización

NOTA 1 Los ejercicios se pueden usar para validar políticas, planes, procedimientos, entrenamiento, equipos y acuerdos entre organizaciones; suministrar aclaraciones y entrenar personal en cuanto a roles y responsabilidades; mejorar la coordinación entre las organizaciones y comunicaciones; identificar la falta de recursos; mejorar el desempeño individual e identificar las oportunidades de mejora; además, son oportunidad controlada para practicar la improvisación.

NOTA 2 Una prueba es un tipo particular y único de ejercicio, el cual incorpora una expectativa de aprobar o no aprobar el elemento de la meta u objetivo del ejercicio que está planificado.

[Fuente: INTE/ISO 22300]

3.19 incidente
situación que podría ser una interrupción, pérdida, emergencia o crisis, o que puede conducir a ellas.

[Fuente: INTE/ISO 22300]

3.20 infraestructura
sistema de instalaciones, equipos y servicios necesarios para el funcionamiento de una organización

3.21 parte interesada
persona u organización que pueden afectar, ser afectados, o percibirse a sí mismos como afectados por una decisión o actividad.

NOTA Esto puede ser un individuo o grupo que tiene un interés en cualquier decisión o actividad de una organización.

3.22 auditoría interna
auditoría realizada por o en nombre de la propia organización, para la revisión de la gestión o para otros propósitos internos y que podría servir de base para una de declaración de conformidad por la misma organización.

NOTA En muchos casos, particularmente en organizaciones pequeñas, la independencia puede ser demostrada por la liberación de responsabilidad sobre la actividad objeto de auditoría.

3.23 activación
acto de declarar que los acuerdos de la organización sobre continuidad del negocio deben llevarse a la práctica con el fin de continuar la entrega de productos o servicios clave.

3.24 sistema de gestión
conjunto de elementos interrelacionados o que interactúan de una organización para establecer políticas y objetivos, y los procesos para alcanzar dichos objetivos.

NOTA 1 Un sistema de gestión puede abordar una sola disciplina o varias disciplinas.

NOTA 2 Los elementos del sistema son la estructura de la organización, roles y responsabilidades, planificación, operación, entre otras.

NOTA 3 El ámbito de aplicación de un sistema de gestión puede incluir la totalidad de la organización, funciones concretas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones a través de un grupo de las organizaciones.

3.25 interrupción máxima aceptable (por sus siglas en inglés, MAO)
el tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto/servicio o realizar una actividad, lo convierta en inaceptable.

NOTA Ver también el periodo máximo tolerable de interrupción.

3.26 período máximo tolerable de interrupción (por sus siglas en inglés, MTPD)
el tiempo que tomaría para que los efectos adversos que pudieran ocurrir como resultado de no proporcionar un producto/servicio o realizar una actividad, lo convierta en inaceptable.

NOTA Ver también Interrupción máxima aceptable.

3.27 medición
proceso para determinar un valor.

3.28 objetivo mínimo de continuidad del negocio (por sus siglas en inglés, MBCO)
nivel mínimo de servicios o productos que es aceptable para la organización para lograr su objetivo de negocio durante una interrupción.

3.29 seguimiento
determinar el estado de un sistema, un proceso o una actividad.

NOTA Para determinar el estado puede haber una necesidad de controlar, supervisar y observar críticamente.

3.30 acuerdo de ayuda mutua
entendimiento preestablecido entre dos o más entidades, con el fin de brindarse ayuda mutua

[Fuente: INTE/ISO 22300]

3.31 no conformidad
Incumplimiento de un requisito.

[Fuente: INTE/ISO 22300]

3.32 objetivo
resultado a lograrse.

NOTA 1 Un objetivo puede ser estratégico, táctico u operacional.

NOTA 2 Los objetivos se pueden referir a diferentes disciplinas (tales como financieras, de salud y seguridad, y metas ambientales) y se pueden aplicar en diferentes niveles (tales como estratégicos, en toda la organización, proyectos, productos y procesos).

NOTA 3 Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado deseado, un propósito, un criterio operativo, como objetivo la continuidad del negocio o por el uso de otras palabras de significado similar (por ejemplo, fin, meta o destino).

NOTA 4 En el contexto de las normas de sistemas de gestión de la seguridad de la sociedad, los objetivos de seguridad de la sociedad pueden ser establecidos por la organización, coherentes con la política de seguridad de la sociedad, para lograr los resultados específicos.

3.33 organización
persona o grupo de personas con roles y responsabilidades propias, autoridades y relaciones para alcanzar sus objetivos.

NOTA 1 El concepto de organización incluye, pero no se limita a la compañía, corporación, firma, empresa, autoridad, asociación, institución, parte o combinación de los mismos, ya sea incorporada o no, pública o privada.

NOTA 2 Para las organizaciones con más de una operación de negocio, una sola unidad puede ser definida como una organización.

3.34 subcontratar
sacer un acuerdo donde una organización externa realiza parte de la función o procesos de una organización.

NOTA Una organización externa está fuera del alcance del sistema de gestión, aunque la función compartida o proceso tercerizado está dentro del ámbito de aplicación.

3.35 desempeño
resultado medible.

NOTA 1 El desempeño se puede relacionar ya sea con los resultados cuantitativos o cualitativos.

NOTA 2 El desempeño puede referirse a la gestión de las actividades, procesos, productos (incluidos los servicios), los sistemas u organizaciones.

3.36 evaluación del desempeño
proceso de determinación de resultados medibles.

3.37 personal
personas que trabajan para y bajo el control de la organización.

NOTA El concepto de personal incluye, pero no se limita, a los empleados, personal a tiempo parcial y personal interno.

3.38 política
intenciones y orientaciones de una organización tal como son expresadas formalmente por la alta dirección.

3.39 procedimiento
forma especificada para llevar a cabo una actividad o un proceso.

3.40 proceso
conjunto de actividades interrelacionadas o que interactúan, las cuales transforman entradas en salidas.

3.41 productos y servicios
resultados beneficiosos proporcionados por una organización a sus clientes beneficiarios y partes interesadas, por ejemplo, artículos manufacturados, seguros de automóviles y servicio de enfermería para la comunidad.

3.42 actividades priorizadas
actividades a las que se debe dar prioridad después de que ha ocurrido un incidente para mitigar los impactos.

[Fuente: INTE/ISO 22300]

3.43 registro
declaración de los resultados obtenidos o evidencia de las actividades ejecutadas.

3.44 punto Objetivo de Recuperación (por sus siglas en inglés, RPO).
punto en el cual la información utilizada por una actividad debe ser restaurada para permitir la reanudación de la operación.

NOTA También se puede denominar como "Pérdida máxima de datos ".

3.45 tiempo objetivo de recuperación (por sus siglas en inglés, RTO)
período de tiempo después de un incidente en el que:
- El producto o servicio debe ser reanudado, o
- La actividad debe reanudarse, o
- Los recursos deben ser recuperados.

NOTA Para los productos, servicios y actividades, el tiempo objetivo de recuperación debe ser menor que el tiempo que tomaría para los efectos adversos que pudieran surgir como consecuencia de no proporcionar un producto/servicio o la realización de una actividad para convertirse en inaceptable.

3.46 requisito
necesidad o expectativa establecida, generalmente implícita u obligatoria.

NOTA 1 "Generalmente implícita" significa que se trata de una costumbre o práctica común para la organización y las partes interesadas que la necesidad o expectativa bajo consideración está implícita.

NOTA 2 Un requisito especificado es aquel que se declara, por ejemplo, en información documentada.

3.47 recursos
todos los activos, recursos humanos, conocimientos, información, tecnología (incluidas las instalaciones y equipos), locales, y suministros e información (ya sean o no electrónicos) que una organización tiene que tener disponibles para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.

3.48 riesgo
efecto de la incertidumbre sobre los objetivos

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 Los objetivos pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso o de una organización completa).

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a potenciales eventos y a sus consecuencias, o a una combinación de ambos.

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las consecuencias de un evento (incluyendo los cambios en las circunstancias) y de su posibilidad.

NOTA 5 La incertidumbre es el estado, incluso parcial, de la deficiencia en la información relacionada con la comprensión o al conocimiento de un evento, de sus consecuencias o de su probabilidad.

[FUENTE: GUÍA INTE/ISO 73]

3.49 apetito de riesgo
es el nivel y tipo de riesgo que la organización está dispuesta a asumir

3.50 valoración del riesgo
proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

[FUENTE: GUÍA INTE/ISO 73]

3.51 gestión del riesgo
actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

[FUENTE: GUÍA INTE/ISO 73]

3.52 poner a prueba
Procedimiento para determinar la presencia, cualidad o veracidad de algo.

NOTA 1 Poner a prueba se puede denominar “ensayo”.

NOTA 2 Las puestas a prueba se aplican con frecuencia a los planes de apoyo.

[Fuente: INTE/ISO 22300]

3.53 Alta dirección
Persona o grupo de personas que dirige y controla a una organización al más alto nivel.

NOTA 1 La alta dirección tiene la facultad de delegar autoridad y proporcionar los recursos dentro de la organización.

NOTA 2 Si el alcance del sistema de gestión cubre únicamente parte de una organización entonces la alta dirección se refiere a quienes dirigen y controlan esa parte de la organización.

3.54 Verificación
Confirmación, a través de la presentación de evidencias, que los requisitos específicos han sido cumplidos.

3.55 Ambiente de trabajo
Conjunto de condiciones bajo las cuales se lleva a cabo el trabajo

NOTA Las condiciones incluyen factores físicos, sociales, psicológicos y ambientales tales como temperatura, esquemas de reconocimiento, ergonómicos y composición atmosférica.

[FUENTE: INTE/ISO 22300]

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 Entendiendo la organización y su contexto

La organización debe determinar los aspectos externos e internos que son pertinentes a su propósito y los que afectan su capacidad para lograr los resultados esperados de su SGCN.

Estos aspectos deben ser tomados en cuenta para establecer, implementar y mantener el SGCN de la organización.

La organización debe identificar y documentar lo siguiente:

a) Las actividades, funciones, servicios, productos, asociaciones, cadenas de suministro, las relaciones con las partes interesadas, y el impacto potencial relacionado con un incidente disruptivo de la organización;

b) Las relaciones entre la política de continuidad del negocio y objetivos de la organización y de otras políticas, incluyendo la estrategia de gestión de riesgo global, y

c) El apetito del riesgo de la organización.

Al establecer el contexto, la organización debe:

1) Articular sus objetivos, incluidos los relativos a la continuidad del negocio,

2) Definir los factores externos e internos que generan la incertidumbre que aumenta el riesgo,

3) Establecer criterios de riesgo, teniendo en cuenta el apetito de riesgo, y

4) Definir el propósito del SGCN.

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 pertinentes al SGCN, y

b) Los requisitos de estas partes interesadas (por ejemplo, si sus necesidades y expectativas están establecidas, generalmente implícitas u obligatorias).

4.2.2 Requisitos legales y reglamentarios

La organización debe establecer, implementar y mantener procedimientos para identificar, tener acceso a, y evaluar los requisitos legales y reglamentarios aplicables a la organización, relacionados con la continuidad de sus operaciones, productos y servicios, así como los intereses de las partes interesadas pertinentes.

La organización debe asegurarse de que estos requisitos legales aplicables, reglamentarios y otros que la organización suscriba se tengan en cuenta para establecer, implementar y mantener su SGCN.

La organización debe documentar esta información y mantenerla actualizada. Novedades o modificaciones legales, reglamentarias, y otros requisitos deben ser comunicados a los empleados afectados y otras partes interesadas.

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

4.3.1 Generalidades

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

Cuando se determine el alcance, la organización debe considerar:

- los aspectos internos y externos a que se refiere en el apartado 4.1, y
- los requisitos mencionados en el apartado 4.2.

El alcance debe estar disponible como información documentada

4.3.2 Alcance del SGCN

La organización debe:

a) Establecer las partes de la organización para ser incluidas en el SGCN,

b) Establecer los requisitos de SGCN, teniendo en cuenta la misión, las metas, las obligaciones internas y externas (incluyendo aquellos relacionados con las partes interesadas), y las responsabilidades legales y reglamentarias de la organización,

c) Identificar los productos, servicios y todas las actividades relacionadas con el alcance del SGCN,

d) Tener en cuenta las necesidades e intereses de las partes interesadas, tales como clientes, inversionistas, accionistas, la cadena de suministro, del público y/o de la comunidad y sus necesidades, expectativas e intereses (según corresponda),

e) Definir el alcance del SGCN en términos apropiados al tamaño, la naturaleza y complejidad de la organización.

Al definir el alcance, la organización debe documentar y explicar las exclusiones; cualquiera de tales exclusiones no debe afectar la capacidad de la organización y la responsabilidad de proveer la continuidad del negocio y las operaciones que se encuentran en los requisitos del SGCN, según lo determinado por el análisis de impacto al negocio o la valoración del riesgo y los requisitos legales y reglamentarios aplicables.

4.4 Sistema de gestión de continuidad del negocio

La organización debe establecer, implementar, mantener y mejorar continuamente un SGCN, incluyendo los procesos necesarios y sus interacciones, en conformidad con los requisitos de esta norma internacional.

5 LIDERAZGO

5.1 Liderazgo y compromiso

Las personas de la alta dirección y otros roles directivos pertinentes de la organización deben demostrar liderazgo con respecto al SGCN.

EJEMPLO Este liderazgo y compromiso puede demostrarse mediante la motivación y el empoderamiento de las personas para contribuir a la eficacia del SGCN.

5.2 Compromiso de la dirección

La alta dirección debe demostrar su liderazgo y compromiso respecto al SGCN:

- Asegurando que las políticas y objetivos son establecidos para el SGCN y son compatibles con la dirección estratégica de la organización,

- Asegurando la integración de los requisitos del SGCN en los procesos del negocio de la organización,
- Asegurando que los recursos necesarios para el SGCN están disponibles,

- Comunicando la importancia de la gestión efectiva de la continuidad del negocio y conforme a los requisitos del SGCN,

- Garantizando que el SGCN logre los resultados esperados,

- Dando dirección y apoyo a las personas que contribuyen a la eficacia del SGCN,

- Promoviendo la mejora continua, y,

- Apoyando otros roles directivos pertinentes para demostrar su liderazgo y compromiso cuando aplique en sus áreas de responsabilidad

NOTA 1 La referencia “negocio" en esta norma internacional es para interpretarse en el sentido amplio de aquellas actividades que son fundamentales para los propósitos de la existencia de la organización.

La alta dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGCN:

- Estableciendo una política de continuidad del negocio,

- Asegurando que los objetivos y planes de SGCN son establecidos,
- Estableciendo roles, responsabilidades y competencias para la gestión de la continuidad del negocio, y

- Designando una o más personas como responsables del SGCN con la autoridad apropiada y competencias necesarias para la implementación y mantenimiento del SGCN.

NOTA 2 Estas personas pueden tener otras responsabilidades dentro de la organización.

La alta dirección debe asegurarse que las responsabilidades y autoridades para las roles pertinentes son asignadas y comunicadas dentro de la organización:

- Definiendo los criterios para la aceptación de riesgos y los niveles de riesgo aceptables,
- Participando activamente en ejercicios y puestas a prueba,

- Asegurando que las auditorías internas del SGCN se llevan a cabo,
- Llevando a cabo la revisión por parte de la alta dirección del SGCN, y
- Demostrando su compromiso con la mejora continua.

5.3 Política

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

a) Sea adecuada para el propósito de la organización,
b) Proporcione el marco de referencia para establecer objetivos de continuidad del negocio,
c) Incluya un compromiso para satisfacer los requisitos aplicables,
d) Incluya un compromiso de mejora continua del SGCN.

La política del SGCN debe:
- estar disponible como información documentada,
- ser comunicada dentro de la organización,
- estar disponible para las partes interesadas, según sea apropiado
- ser revisada para su continua adecuación a intervalos definidos y cuando se produzcan cambios significativos.

La organización debe conservar información documentada sobre la política de continuidad del negocio.

5.4 Roles, responsabilidades y autoridades

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes sean asignadas y comunicadas dentro de la organización.

La alta dirección debe asignar la responsabilidad y autoridad para:

a) Asegurar que el sistema de gestión se establezca en conformidad con los requisitos de esta norma internacional, e,
b) Informar sobre el desempeño del SGCN a la alta dirección.

6 PLANIFICACIÓN

6.1 Acciones para tratar riesgos y oportunidades

Cuando se haga la planeación del SCGN, la organización debe considerar los aspectos mencionados en el apartado 4.1 y los requisitos contemplados en el apartado 4.2 y determinar los riesgos y oportunidades que necesitan ser dirigidas a:

a) Asegurar que el sistema de gestión puede lograr los resultados deseados,
b) Prevenir o reducir los efectos no deseados, y
c) Lograr el mejoramiento continuo,

La organización debe planear:
a) Las acciones para tratar estos riesgos y oportunidades,
b) Cómo:
   1) Integrar e implementar las acciones dentro de sus procesos de SGCN (véase apartado 8.1)
   2) Evaluar la eficacia de éstas acciones

6.2 Objetivos de continuidad del negocio y planes para alcanzarlos

La alta dirección debe asegurar que los objetivos de continuidad del negocio son establecidos y comunicados para las funciones y niveles pertinentes dentro de la organización.

Los objetivos de continuidad del negocio deben:

a) Ser coherentes con la política de continuidad del negocio,
b) Tener en cuenta el nivel mínimo de productos y servicios que sea aceptable para que la organización logre sus objetivos.
c) Ser medibles,
d) Tener en cuenta los requisitos aplicables, y
e) Controlarse y actualizarse según corresponda.

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

Para lograr sus objetivos de continuidad del negocio, la organización debe determinar:
- Quien será el responsable,
- Que se hará,
- Qué recursos serán requeridos,
- Cuando serán completados, y,
- Cómo serán evaluados los resultados.

7 SOPORTE

7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGCN.

7.2 Competencia

La organización debe:

a) Determinar las competencias necesarias del personal para hacer el trabajo que afecta su desempeño,
b) Asegurarse que estas personas son competentes sobre la base de una educación adecuada, entrenamiento y experiencia,
c) Cuando sea aplicable, tomar medidas para adquirir la competencia necesaria, y evaluar la eficacia de las medidas adoptadas, y
d) Mantener información documentada apropiada como evidencia de la competencia.

NOTA Las acciones aplicables pueden incluir, por ejemplo: la provisión de entrenamiento para la tutoría, o cambio de destino de los empleados actuales, o la contratación de personas competentes.

7.3 Toma de conciencia

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

a) La política de continuidad del negocio,
b) Su contribución a la eficacia del SGCN, incluyendo los beneficios de la mejora del desempeño de la Gestión de continuidad del negocio,

c) Las implicaciones de las no conformidades con los requisitos del SGCN, y
d) Su propio rol ante un incidente disruptivo.

7.4 Comunicación

La organización debe determinar la necesidad de comunicación interna y externa correspondiente al SGCN, incluyendo:

a) qué se comunicará
b) cuando comunicar
c) a quienes comunicar

La organización debe establecer, implementar y mantener procedimientos para:
- La comunicación interna entre las partes interesadas y los empleados dentro de la organización,
- La comunicación externa con los clientes, las entidades asociadas, la comunidad local, y otras partes interesadas, incluyendo los medios de comunicación,
- Recibir, documentar y responder a las comunicaciones de las partes interesadas,
- La adaptación y la integración de un sistema de alerta de amenaza nacional o regional, o su equivalente, en la planificación y uso operativo, si aplica,
- Asegurar la disponibilidad de los medios de comunicación durante un incidente disruptivo,
- Facilitar la comunicación estructurada con las autoridades competentes y garantizar la interoperabilidad de las varias organizaciones y el personal.
- Las operaciones y puestas a prueba de las capacidades de comunicación destinadas a ser utilizadas durante la interrupción de la normalidad en las comunicaciones.

NOTA Otros requisitos para la comunicación en respuesta a un incidente se especifican en el apartado 8.4.3

7.5 Información documentada

7.5.1 Generalidades

El SGCN de la organización debe incluir:
- La información documentada requerida por esta norma internacional, y
- La información documentada determinada por la organización como necesaria para la eficacia de los SGCN.

NOTA El alcance de la información documentada para un SGCN puede diferir de una organización a otra debido a:

- El tamaño de la organización y su tipo de actividades, procesos, productos y servicios,
- La complejidad de los procesos y sus interacciones, y
- La competencia de las personas.

7.5.2 Creación y actualización

Cuando se crea y actualiza la información documentada, asegurarse de que lo siguiente sea apropiado:

a) La identificación y descripción (por ejemplo, un título, nombre, fecha, autor, número), y
b) Formato (por ejemplo, el idioma, la versión de software, gráficos) y los medios de comunicación (por ejemplo, papel, electrónico).

7.5.3 Control de la información documentada

La información documentada requerida por el SGCN y por esta norma debe ser controlada para asegurar que:

a) Está disponible y es apropiada para el uso, donde y cuando sea necesario,
b) Está adecuadamente protegida (por ejemplo, de pérdida de confidencialidad, uso inapropiado, o pérdida de la integridad)

Para el control de la información documentada, la organización debe orientarse a las siguientes actividades, cuando sea aplicable:
- Distribución, acceso, recuperación y uso,
- Almacenamiento y conservación, incluyendo preservación de la legibilidad (es decir, lo suficientemente claro para leer),
- Control de cambios (por ejemplo, control de versiones),
- Retención y eliminación,
- Prevención del uso no intencionado de la información obsoleta.

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

Al establecer el control de la información documentada, la organización debe asegurarse de que existe una protección adecuada de la información documentada (por ejemplo, protección contra el compromiso, la modificación o supresión no autorizada).

NOTA El acceso implica una decisión sobre el permiso para ver la información documentada, o el permiso de la autoridad para ver y cambiar la información documentada, etc.

8 OPERACIÓN

8.1 Planificación y control operacional

La organización debe planear, implementar, y controlar los procesos necesarios para cumplir los requisitos para ejecutar las acciones determinadas en el apartado 6.1, para:
a) Establecer los criterios para esos procesos,
b) Implementar el control de estos procesos de acuerdo con los criterios, y
c) Mantener información documentada, según sea necesario, para tener la confianza en que los procesos se han llevado a cabo como estaba previsto.

La organización debe controlar los cambios previstos y revisar las consecuencias de los cambios no deseados, tomando acciones para mitigar los efectos adversos, según sea necesario.

La organización debe asegurar que los procesos subcontratados sean controlados.

8.2 Análisis de impacto al negocio y valoración del riesgo

8.2.1 Generalidades

La organización debe establecer, implementar y mantener un proceso formal y documentado para el análisis de impacto al negocio y valoración del riesgo, que:

a) Establezca el contexto de la valoración, defina los criterios y evalúe el impacto potencial de un incidente disruptivo,
b) Tome en cuenta los requisitos legales y otros requisitos que la organización suscriba,
c) Incluya un análisis sistemático, la priorización de los tratamientos del riesgo, y sus costos relacionados,

d) Defina la salida necesaria del análisis de impacto al negocio y valoración del riesgo, y
e) Especifique los requisitos para que esta información se mantenga actualizada y confidencial.

NOTA Existen diversas metodologías para análisis de impacto al negocio y la valoración del riesgo que determinará el orden en que éstas se llevarán a cabo.

8.2.2 Análisis de impacto al negocio

La organización debe establecer, implementar y mantener un proceso de evaluación formal y documentado para la determinación de la continuidad y la recuperación de las prioridades, objetivos y metas. Este proceso debe incluir la evaluación de impactos de las actividades disruptivas que soportan a los productos y servicios de la organización.

El análisis de impacto al negocio debe incluir lo siguiente:

a) La identificación de actividades que soportan la prestación de bienes y servicios;
b) La evaluación de los impactos en el tiempo de no realizar estas actividades;
c) El establecimiento de plazos prioritarios para la reanudación de estas actividades a un nivel mínimo especificado aceptable, tomando en cuenta el tiempo en que los impactos de la no reanudación de éstas llegarían a ser inaceptables, y
d) La identificación de dependencias y recursos de soporte para estas actividades, incluyendo proveedores, subcontratados, socios y otras partes interesadas pertinentes.

8.2.3 Valoración del riesgo

La organización debe establecer, implementar y mantener un proceso formal de valoración del riesgo documentado que sistemáticamente identifica, analiza y evalúa el riesgo de incidentes disruptivos a la organización.

NOTA Este proceso puede realizarse de acuerdo con la norma INTE/ISO 31000.

La organización debe:
a) Identificar los riesgos de la interrupción de las actividades prioritarias de la organización y los procesos, sistemas, información, personas, activos, proveedores y otros recursos que los soportan,
b) Analizar sistemáticamente el riesgo,
c) Evaluar cuales riesgos relacionados con la interrupción requieren tratamiento, e
d) Identificar tratamientos acordes con los objetivos de continuidad del negocio y de acuerdo con el apetito del riesgo de la organización.

NOTA La organización debe ser consciente de que ciertas obligaciones financieras o gubernamentales requieren la comunicación de estos riesgos a diferentes niveles de detalle. Además, ciertas necesidades de la sociedad también pueden garantizar el intercambio de esta información en un nivel adecuado de detalle.

8.3 Estrategia de continuidad del negocio

8.3.1 Determinación y selección

La determinación y selección de la estrategia se debe basar en los resultados de los análisis de impacto al negocio y valoración del riesgo.

La organización debe determinar una estrategia de continuidad del negocio apropiada para:

a) La protección de las actividades prioritarias,
b) La estabilización, continuación, reanudación y recuperación de las actividades prioritarias y sus dependencias y recursos de soporte, y,
c) La mitigación, respuesta y gestión de los impactos.

La determinación de la estrategia debe incluir la aprobación de plazos priorizados para la reanudación de las actividades.

La organización debe llevar a cabo evaluaciones de las capacidades de continuidad del negocio de los proveedores.

8.3.2 Establecimiento de los recursos requeridos

La organización debe determinar los recursos requeridos para implementar las estrategias seleccionadas. Los tipos de recursos considerados se incluyen, pero no se limitan a:

a) las personas,
b) la información y los datos,
c) Los edificios, el ambiente de trabajo y servicios asociados,
d) Instalaciones, equipos y consumibles,
e) el sistema de información y la tecnología de la comunicación (TIC)
f) el transporte
g) la financiación, y,
h) socios y proveedores.

8.3.3 Protección y mitigación

Para los riesgos identificados que requieren tratamiento, la organización debe considerar medidas proactivas que:

a) Reduzcan la posibilidad de interrupción,
b) Acorten el período de interrupción, y,
c) Limiten el impacto de la interrupción de los productos y servicios clave de la organización.

La organización debe elegir e implementar los tratamientos del riesgo adecuados de acuerdo con su apetito del riesgo.

8.4 Establecer e implementar procedimientos de continuidad del negocio

8.4.1 Generalidades

La organización debe establecer, implementar y mantener procedimientos de continuidad del negocio para gestionar un incidente disruptivo y continuar con sus actividades basadas en los objetivos de recuperación identificadas en el análisis de impacto al negocio.

La organización debe documentar los procedimientos (incluidos los acuerdos necesarios) para asegurar la continuidad de actividades y la gestión de un incidente disruptivo.

Los procedimientos deben:
a) establecer un protocolo de comunicaciones interno y externo adecuado,
b) ser específicos con respecto a las medidas inmediatas que deben tomarse durante una interrupción,
c) ser flexibles para responder a amenazas imprevistas y las cambiantes condiciones internas y externas,
d) centrarse en el impacto de los eventos que podrían potencialmente interrumpir las operaciones,
e) ser desarrollados con base a los supuestos establecidos y el análisis de las interdependencias,
f) ser eficaz en la reducción de sus consecuencias a través de la aplicación de estrategias apropiadas de mitigación.

8.4.2 Estructura de respuesta ante incidentes

La organización debe establecer, documentar e implementar procedimientos y una estructura de gestión para responder ante un incidente disruptivo con el uso del personal con la debida responsabilidad, autoridad y competencia para manejar un incidente.

La estructura de respuesta debe:

a) Identificar los umbrales de los efectos que justifiquen la iniciación de la respuesta formal,
b) Evaluar la naturaleza y el alcance de un incidente disruptivo y su impacto potencial,
c) Activar una respuesta apropiada de continuidad del negocio,
d) Tener procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta,
e) Tener los recursos disponibles para soportar los procesos y procedimientos para gestionar un incidente disruptivo para minimizar el impacto, y,
f) Comunicarse con las partes interesadas y las autoridades, así como, con los medios de comunicación.

La organización debe decidir, asegurando la vida humana como primera prioridad y en consulta con las partes interesadas, si se comunica externamente la información acerca de sus riesgos e impactos significativos y documentar su decisión. Si la decisión es comunicarla, entonces, la organización debe establecer e implementar procedimientos para la comunicación externa, alertas y advertencias, incluyendo los medios de comunicación, según corresponda.

8.4.3 Advertencia y comunicación

La organización debe establecer, implementar y mantener procedimientos para:

a) La detección de un incidente,
b) El seguimiento regular de un incidente,
c) La comunicación interna dentro de la organización y recepción, documentación y respuesta a las comunicaciones de las partes interesadas,
d) Recibir, documentar y responder a cualquier sistema de alerta de riesgo a nivel nacional o regional o su equivalente,
e) Asegurar la disponibilidad de los medios de comunicación durante un incidente disruptivo,
f) Facilitar la comunicación estructurada con los servicios de emergencia,
g) Registrar la información vital sobre el incidente, las medidas adoptadas y las decisiones tomadas. Lo siguiente debe ser considerado e implementado, cuando sea aplicable:

- Alerta a las partes interesadas potencialmente afectadas por un incidente disruptivo real o inminente;

- Aseguramiento de la interoperabilidad de múltiples organizaciones y del personal;

- Operación de una instalación de comunicaciones.

Los procedimientos de comunicación y de alerta deben ser ejercitados regularmente.

8.4.4 Planes de continuidad del negocio

La organización debe establecer procedimientos documentados para responder a un incidente disruptivo y cómo continuará o recuperará sus actividades dentro de un plazo predeterminado. Los procedimientos deben dirigir los requisitos a aquellos quienes van a usarlos.

Los planes de continuidad del negocio deben contener colectivamente:

a) Los roles y responsabilidades definidos para las personas y los equipos que tienen autoridad durante y después de un incidente,

b) Un proceso para la activación de la respuesta,

c) Los detalles para gestionar las consecuencias inmediatas de un incidente disruptivo, teniendo en cuenta:

1) El bienestar de los individuos,
2) Las opciones estratégicas, tácticas y operativas para la respuesta a la interrupción, y
3) La prevención de la pérdida o no disponibilidad de las actividades prioritarias;

d) La información detallada sobre cómo y bajo qué circunstancias la organización se comunicará con los empleados y sus familiares, las partes interesadas claves y los contactos de emergencia,

e) Cómo la organización va a continuar o recuperar sus actividades prioritarias dentro de los plazos predeterminados,

f) Los detalles de la respuesta de la organización a los medios de comunicación a raíz de un incidente, incluyendo:
1) una estrategia de comunicación,
2) la interfaz seleccionada con los medios de comunicación,
3) guía o plantilla para la redacción de una declaración para los medios de comunicación, y
4) portavoces apropiados;

g) un proceso para finalizar una vez que el incidente ha terminado

Cada plan debe definir
- propósito y alcance,
- objetivos,
- criterios y procedimientos de activación,
- procedimientos de implementación,
- roles, responsabilidades y autoridades,
- requisitos y procedimientos de comunicación,
- interdependencias internas y externas y las interacciones,
- necesidades de recursos, y
- flujo de información y procesos de documentación.

8.4.5 Recuperación

La organización debe tener procedimientos documentados para restaurar y retornar a las actividades del negocio desde las medidas adoptadas temporalmente para soportar los requisitos normales del negocio después de un incidente.

8.5 Ejercicios y puestas a prueba

La organización debe practicar y probar sus procedimientos de continuidad del negocio para asegurar que sean compatibles con sus objetivos de continuidad del negocio.

La organización debe llevar a cabo prácticas y pruebas que:

a) Sean coherentes con el alcance y los objetivos del SGCN,
b) Sean basados en escenarios apropiados que estén bien planificados, con objetivos y fines claramente definidos,

c) En el transcurso del tiempo, sean validados en conjunto la totalidad de los acuerdos de continuidad del negocio, involucrando las partes interesadas pertinentes,
d) Reduzcan al mínimo el riesgo de interrupción de las operaciones,
e) Produzcan posterior a la práctica informes formales que contengan resultados, recomendaciones y acciones para implementar mejoras
f) Sean revisados en el contexto de promover la mejora continua, y
g) Sean llevados a cabo a intervalos planificados, y cuando hayan cambios significativos dentro de la organización o en el entorno en el que opera.

9 EVALUACIÓN DEL DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

9.1.1 Generalidades

La organización debe determinar:

a) a qué es necesario dar seguimiento y qué es necesario medir;
b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar la validez de los resultados,
c) cuándo el seguimiento y la medición se llevarán a cabo, y
d) cuándo los resultados del seguimiento y medición deben ser analizados y evaluados.

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

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

Adicionalmente, la organización debe

- tomar acciones cuando sea necesario para hacer frente a las tendencias o resultados adversos antes de que se presente una no conformidad, y
- conservar la información documentada pertinente como evidencia de los resultados.

Los procedimientos para el seguimiento del desempeño deben proveer el:
- establecimiento de indicadores de desempeño adecuados a las necesidades de la organización,
- seguimiento del alcance en que se cumplan las políticas, los objetivos y las metas de continuidad del negocio de la organización,
- desempeño de los procesos, procedimientos y funciones que protegen sus actividades prioritarias,
- seguimiento del cumplimiento con esta norma y con los objetivos de continuidad del negocio,
- seguimiento de la evidencia histórica de los resultados deficientes del desempeño del SGCN, y
- registro de datos y resultados de seguimiento y medición para facilitar acciones correctivas subsecuentes.

NOTA El desempeño deficiente puede incluir las no conformidades, cuasi accidentes, falsas alarmas e incidentes reales.

9.1.2 Evaluación de los procedimientos de continuidad del negocio

a) La organización debe llevar a cabo evaluaciones de sus procedimientos de continuidad del negocio y capacidades para asegurar su continua adecuación, idoneidad y eficacia;

b) Estas evaluaciones deben llevarse a cabo a través de revisiones periódicas, ejercicios, puestas a prueba, reportes después de incidentes y evaluaciones del desempeño. Los cambios significativos que surjan deben ser reflejados en los procedimientos de manera oportuna;

c) La organización debe evaluar periódicamente el cumplimiento con los requisitos legales y reglamentarios aplicables, mejores prácticas de la industria, y la conformidad con su propia política y objetivos de continuidad del negocio, y

d) La organización debe llevar a cabo evaluaciones a intervalos planificados y cuando se produzcan cambios significativos.

Cuando un incidente disruptivo ocurra y resulte en la activación de sus procedimientos de continuidad del negocio, la organización debe realizar una revisión posterior al incidente y registrar los resultados.

9.2 Auditoría interna

La organización debe realizar auditorías internas a intervalos planificados para proporcionar información si el SGCN:
a) Se ajusta a:
1) los requisitos propios de la organización para su SGCN, y
2) los requisitos de esta norma internacional,

b) Es eficazmente implementado y mantenido

La organización debe:
- planear, establecer, implementar y mantener un programa de auditoría, incluyendo la frecuencia, los métodos, las responsabilidades, los requisitos de planificación y la realización de informes. El programa de auditoría debe tener en consideración la importancia de los procesos y de los resultados de auditorías anteriores,
- definir los criterios de auditoría y el alcance de cada una,
- seleccionar auditores y gestionar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría,
- garantizar que los resultados de las auditorías son informados a la dirección, y
- mantener información documentada como evidencia de la implementación del programa de auditoría y de sus resultados.

El programa de auditoría, incluyendo cualquier programación, debe basarse en los resultados de la valoración del riesgo de las actividades de la organización y los resultados de auditorías anteriores. Los procesos de auditoría deben cubrir el alcance, frecuencia, metodologías y competencias, así como las responsabilidades y requisitos para la realización de auditorías e informar de los resultados de verificación.

La dirección responsable del área que está siendo auditada debe asegurarse que cualquier corrección necesaria y cualquier acción correctiva se toman sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones tomadas y su informe de resultados.

9.3 Revisión por la dirección

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

La revisión por la dirección debe considerar:

a) el estado de las acciones de las revisiones previas por la dirección,
b) los cambios en los asuntos internos y externos que son pertinentes para el SGCN,
c) información sobre el desempeño de la continuidad del negocio, incluyendo las tendencias en:

1) no conformidades y acciones correctivas,
2) resultados del seguimiento y la evaluación, y
3) resultados de auditoría,

d) las oportunidades para la mejora continua.

Las revisiones por la dirección deben considerar el desempeño de la organización, incluyendo:

- acciones de seguimiento de las revisiones anteriores por la dirección,
- necesidad de cambios en el SGCN, incluyendo la política y los objetivos,
- oportunidades de mejora,
- resultados de las auditorías y revisiones al SGCN, incluidos los de los principales proveedores y socios, cuando aplique,
- técnicas, productos o procedimientos, que pueden ser utilizados en la organización para mejorar el desempeño y eficacia del SGCN,
- estado de las acciones correctivas,
- resultados de ejercicios y puestas a prueba,
- riesgos o asuntos no abordados adecuadamente en cualquier valoración del riesgo anterior,
- cualquier cambio que pudiera afectar el SGCN, ya sea interno o externo al alcance del SGCN,
- adecuación de la política,
- recomendaciones de mejora,
- lecciones aprendidas y las acciones derivadas de incidentes disruptivos, y
- buenas prácticas y guías que surjan.

El resultado de la revisión por la dirección debe incluir decisiones relacionadas con oportunidades de mejora continua y la posible necesidad de cambios al SGCN e incluyen lo siguiente:

a) variaciones en el alcance del SGCN;
b) mejoramiento de la eficacia del SGCN;
c) actualización de la valoración del riesgo, análisis de impacto al negocio, planes de continuidad del negocio y los procedimientos relacionados;
d) modificación de los procedimientos y controles para responder a los eventos internos o externos que pueden afectar al SGCN incluyendo cambios a:

1) los requisitos del negocio y operacionales,
2) reducción del riesgo y requisitos de seguridad[1],
3) condiciones y procesos de operación,
4) requisitos legales y reglamentarios,
5) obligaciones contractuales,
6) niveles de riesgo y/o criterios de aceptación de riesgos,
7) necesidades de recursos,
8) financiación y necesidades presupuestarias,

e) cómo la eficacia de los controles es medida.

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

La organización debe:

- comunicar los resultados de la revisión de la gestión a las partes interesadas pertinentes, y
- tomar las medidas apropiadas en relación con esos resultados.

[1] Nota Nacional: En esta norma nacional los términos en ingles de "*security"* y "*safety"* se traducen como seguridad y seguridad humana respectivamente, debido a que son dos términos distintos.

10 MEJORA

10.1 No conformidad y acción correctiva

Cuando ocurra una no conformidad, la organización debe:

a) identificar la no conformidad, y
b) responder a la no conformidad, y, cuando aplique:
    1) tomar medidas para controlarla y corregirla, y,
    2) ocuparse de las consecuencias.

c) evaluar la necesidad de adoptar medidas para eliminar las causas de la no conformidad, para que así no se repita o se produzca en otra parte, que incluya:
    1) revisar las no conformidades,
    2) determinar las causas de no conformidades,
    3) determinar la existencia de no conformidades similares, o que potencialmente pudieran ocurrir,
    4) evaluar la necesidad de acciones correctivas para asegurar que las no conformidades no se repitan o se produzcan en otros lugares,
    5) determinar e implementar las acciones correctivas necesarias,
    6) revisar la eficacia de cualquier acción correctiva tomada, y
    7) aplicar los cambios al SGCN, si es necesario.
d) implementar cualquier acción requerida,
e) revisar la eficacia de cualquier acción tomada,
f) hacer cambios al SGCN, si es necesario.

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

La organización debe mantener la información documentada como evidencia de:

- la naturaleza de las no conformidades y de cualquier acción tomada a futuro, y
- los resultados de cualquier acción correctiva.

10.2 Mejora continua

La organización debe mejorar continuamente la idoneidad, adecuación o eficacia del SGCN.

NOTA La organización puede utilizar los procesos del SGCN tales como el liderazgo, planeamiento y evaluación del desempeño, para lograr una mejora.

11 CORRESPONDENCIA

Esta norma nacional idéntica a la norma internacional **ISO 22301:2012**, " Societal security — Business continuity management systems — Requirements".

BIBLIOGRAFÍA

[1] INTE/ISO 9001, *Sistemas de gestión de la calidad - Requisitos*

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

[3] INTE/ISO 19011, *Directrices para la auditoría de los sistemas de gestión.*

[4] INTE/ISO/IEC 20000-1, *Tecnología de la información - Gestión del servicio. Parte 1: Especificaciones.*

[5] INTE/ISO 22300, *Seguridad de la sociedad — Terminologia*

[6] ISO/PAS 22399, *Societal security — Guideline for incident preparedness and operational continuity management*

[7] ISO/IEC 24762, *Information technology — Security techniques — Guidelines for Information and communications technology disaster recovery services*

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

[9] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] INTE/ISO 31000, *Gestión del riesgo. Principios y directrices*

[11] INTE/ISO/IEC 31010, *Gestión del riesgo. Técnicas de valoración del riesgo.*

[12] INTE/ISO/IEC Guide 73, Gestión del riesgo. Vocabulario

[13] INTE 01-01-18-2011 Parte I Gestión de Continuidad de negocio. Parte 1: Código de práctica

[14] INTE 01-01-18-2011 Parte II, Gestión de la Continuidad del negocio. Parte 2: Requisitos

[15] SI 24001, *Security and continuity management systems — Requirements and guidance for use*, Standards Institution of Israel

[16] NFPA 1600, *Standard on disaster/emergency management and business continuity programs*, National Fire Protection Association (USA)

[17] *Business Continuity Plan Drafting Guideline*, Ministry of Economy, Trade and Industry (Japan), 2005

[18] *Business Continuity Guideline*, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

[19] ANSI/ASIS SPC.1, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use*

[20] SS 540 : 2008, *Singapore Standard for Business Continuity Management*

[21] ANSI/ASIS/BSI BCM.01, *Business Continuity Management Systems: Requirements with Guidance for Use*