ISO 22301:2019

GUÍA DE IMPLANTACIÓN DE LA CONTINUIDAD DE NEGOCIO

nqa.

> ISO 22301:2019

GUÍA DE IMPLANTACIÓN

Contenido

INTRODUCCIÓN A LA NORMA

La ISO 22301:2019 es la última versión de la norma internacional para sistemas de gestión de la continuidad de negocio (SGCN) y proporciona un marco de buenas prácticas para ayudar a las organizaciones a gestionar eficazmente el impacto de una interrupción en su funcionamiento.

El propósito de la norma no es necesariamente lograr la mitigación total del impacto de la interrupción, sino de ayudar a una organización a comprender la magnitud y el tipo de impacto que está dispuesta a aceptar después de una interrupción para lo cual la organización desarrolla un sistema de continuidad del negocio dimensionado correctamente para sus necesidades.

Muchas organizaciones experimentarán en algún momento una interrupción comercial. La causa y la naturaleza de los eventos disruptivos cambian constantemente. Las organizaciones deben poder pensar de manera dinámica sobre este cambiante panorama de amenazas y poner en marcha planes adecuados para mitigar los impactos.

La familia ISO 22300

El origen de la norma ISO 22301 se remonta al comité técnico ISO/TC 23, que se centró en abordar las preocupaciones relacionadas con la seguridad social. Ahora la norma es gestionada por ISO/TC 292 - Seguridad y resiliencia. La primera versión de la nomar ISO 22301 se publicó en 2012. La segunda edición se publicó en octubre de 2019 y es el tema central de esta guía de implantación.

Actualmente existen 11 normas en la serie ISO 22300. Dichas normas brindan orientación y requisitos más detallados para cuestiones específicas relacionadas con la continuidad del negocio. Esto va desde la gestión de respuesta a emergencias, hasta las evacuaciones masivas.

Revisiones y actualizaciones

Las normas ISO están sujetas a revisión aproximadamente cada cinco años para evaluar si se requiere de una actualización.

La actualización más reciente de la norma ISO 22301 en 2019 provocó una serie de cambios. Si bien la edición anterior (2012) fue una de las precursoras en la adopción de un formato tipo Anexo SL, la nueva edición alinea firmemente la norma con el Anexo SL.

La versión 2019 de la norma refleja el movimiento más amplio de las normas ISO hacia la aplicación del pensamiento basado en el riesgo, la comprensión del contexto organizacional y la satisfacción de las necesidades de las partes interesadas. La versión 2019 contiene requisitos menos prescriptivos y es más flexible en su enfoque de la información documentada. La versión 2019 incluye además el nuevo requisito de planificar de manera efectiva los cambios en el Sistema de Gestión de la Continuidad de Negocio (SGCN).

Dentro de la serie, las nomas más importantes para una organización que busque implementar un SGCN efectivo son:

- **ISO 22300:2018 - Seguridad y resiliencia**
  - Vocabulario
- **ISO 22301:2019 - Seguridad y resiliencia**
  - Sistema de Gestión de Continuidad de Negocio
  - Requisitos
- **ISO 22313:2020 - Seguridad y resiliencia**
  - Sistema de Gestión de Continuidad de Negocio
  - Orientación: Proporciona orientación útil en apoyo de la implantación práctica y el funcionamiento de un SGCN.

BENEFICIOS DE LA IMPLANTACIÓN

La capacidad de una empresa para gestionar eventos disruptivos se está volviendo fundamental para su supervivencia. La variedad de amenazas que pueden causar interrupciones comerciales es cada vez mayor. Desde ciberataques y pandemias globales hasta desastres naturales, una organización necesita un conjunto de herramientas para administrarse a sí misma en tiempos de incertidumbre.

En el pasado, la planificación de la continuidad del negocio tendía a estar reservada para la infraestructura nacional crítica y las grandes corporaciones. Hoy en día, la continuidad del negocio es un tema que afecta prácticamente a todas las organizaciones. Un SGCN correctamente implantado debe adaptarse al tamaño y la complejidad de la organización, haciéndolo adecuado tanto para PYMES como para grandes corporaciones.

El propósito principal del SGCN es permitir la mitigación de una interrupción. Dependiendo de la organización, los beneficios funcionarán apoyando sus objetivos; ya sea para salvar vidas en un hospital o para reducir el impacto financiero en una empresa de fabricación.

RESILIENCIA VISIBLE

Un SGCN eficaz proporciona evidencia a los clientes actuales y potenciales de la preparación organizacional para la interrupción. Esto es particularmente importante en sectores donde la disrupción puede tener impactos significativos en la vida de las personas o financieros; incluidos los servicios gubernamentales, sanitarios, financieros, de defensa y sociales.

VENTAJA COMPETITIVA

Poder continuar operando durante o poco después de una interrupción le da a la empresa una ventaja competitiva. A corto plazo, puede obtener negocios frente a competidores que no pueden operar o que lo están haciendo con una capacidad disminuida. A largo plazo, una empresa puede generar beneficios de reputación que atraerá clientes y se beneficiarán de capacidades financieras más sólidas.

Además, un SGCN ayuda a una organización a licitar o licitar de manera más eficaz.

PROTECCIÓN DEL VALOR ORGANIZATIVO

Un SGCN ayuda a mitigar el impacto negativo de un evento disruptivo. En términos prácticos, esto puede ahorrarle a la organización importantes cantidades de dinero, tiempo e impacto en su reputación.

TRANQUILIDAD

El futuro es incierto y un SGCN efectivo brinda a una organización la confianza para avanzar sabiendo que puede gestionar interrupciones. Esta tranquilidad abarca a toda la organización, desde los equipos de operaciones de personal hasta la junta directiva.

MEJORA DE LA CIBERSEGURIDAD Y RESILIENCIA A LA QUIEBRA

La seguridad cibernética y la planificación de desastres de TI ocupan un lugar destacado en la agenda de muchas organizaciones. Un plan de continuidad empresarial ayuda a gestionar el impacto de la interrupción de TI. Esto puede deberse a una acción malintencionada o fallo de la infraestructura. Los virus criptográficos, los ataques DDoS y las fallos del centro de datos pueden crear interrupciones profundas y duraderas en todas las funciones de una organización.

Las certificaciones de seguridad cibernética como la ISO 27001 no abordan completamente los desafíos de continuidad en caso de interrupción. La ISO 27001 intenta abordar la continuidad dentro de la propia función de TI, pero esto no se extiende al resto de la organización. La ISO 22301 proporciona un marco más amplio para abordar el impacto organizacional de fallos de TI. Como resultado, el SGCN (ISO 22301) puede integrarse con un sistema de gestión d seguridad de la información (ISO 27001).

Visión de alto nivel

El SGCN opera con principios similares a otros sistemas de gestión. El sistema se basa en el modelo Planificar-Hacer-Verificar-Actuar (PHVA).

- **Determine las necesidades de la organización y comprenda la justificación de los planes de continuidad de negocio:**
  - ¿Qué es importante continuar en caso de una interrupción?
  - ¿Por qué es importante y para quién?
  - ¿Qué nivel de disrupción están dispuestos a aceptar la organización y sus partes interesadas?
- **Poner en marcha un marco para lograr la mitigación de la interrupción. Esto puede incluir:**
  - Procesos
  - Capacidades
  - Estructuras de respuesta
- **Verificar el rendimiento y la eficacia del sistema mediante el seguimiento. En términos prácticos, esto implicará probar los planes de continuidad de negocio a través de varios medios.**
- **Mejorar el sistema en base a las medidas establecidas, revisar la justificación de los planes de continuidad de negocio y su alineación con lo implementado.**

Uno de los desafíos del SGCN es que entra en acción con poca frecuencia. Si bien los sistemas de gestión de la calidad se implementan en las operaciones diarias de la empresa, los SGCN solo se ponen en marcha por completo cuando se produce una interrupción. Esto significa que debe hacerse mayor hincapié en:

- Pruebas o simulacros del plan de continuidad del negocio.
- Conservación y actualización de las capacidades organizativas para respaldar la continuidad de negocio.
- Revisiones periódicas del sistema, sus procesos y justificación para garantizar que se mantenga alineado con una organización cambiante.

PRINCIPIOS CLAVE DE LA CONTINUIDAD DE NEGOCIO

La continuidad de negocio se basa en una serie de principios clave que deben aplicarse de forma coherente al sistema de gestión de continuidad de negocio para que sea eficaz.

Responsibilidad

La gerencia y la junta directiva de una organización son responsables de la continuidad del negocio, esta debe entenderse y aceptarse. La gestión de la continuidad de negocio debe ser un componente integral de la gestión general de riesgos.

En caso de una interrupción, la ausencia de responsabilidades, autoridades y roles claramente definidos puede hacer que un plan de continuidad del negocio se vuelva ineficaz.

Objetivos claros

Una organización debería tener objetivos claros de continuidad del negocio que reflejen la naturaleza de sus actividades y su impacto en las partes interesadas. Esto respalda la priorización y la asignación de recursos al proceso de continuidad del negocio. Estos objetivos deben definir claramente los niveles de continuidad esperados y los tiempos de continuidad.

Impacto y evaluación de riesgos

La norma de continuidad del negocio es diferente de otros en que se centra en el "qué pasaría si". La capacidad de identificar y planificar los posibles impactos y riesgos comerciales es clave para un sistema de continuidad de negocio eficaz.

Comunicación

Las organizaciones deben incluir en sus planes de continuidad de negocio cómo y cuándo se comunicarán con clientes y partes interesadas (como reguladores o proveedores).

Prueba

El Sistema de gestión de la continuidad de negocio debe probarse periódicamente para evaluar su eficacia y realizar los cambios necesarios.

CICLO PHVA

La ISO 22031 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA), también conocido como círculo Deming o Shewhart. El ciclo PHVA se puede aplicar no solo al sistema de gestión como un todo, sino a cada elemento individual para proporcionar un enfoque continuo en la mejora continua. A modo de resumen:

Planificar

Comprender el contexto y las necesidades externas de las partes interesadas. Identificar riesgo y oportunidad. Establecer objetivos y recursos necesarios.

Hacer

Implementar lo planeado. Desde un nuevo sistema de gestión de la continuidad del negocio hasta pequeños cambios en los procesos.

Verificar

Controlar y medir la efectividad de la continuidad de negocio. Probar los planes de continuidad de negocio y controlar los resultados.

Actuar

Actuar uando sea necesario, basándose en el seguimiento, la medición y otros impulsores de la acción.

PHVA modelo ISO 22301

El modelo PHVA es un ejemplo de sistema de circuito cerrado. Esto asegura que el aprendizaje de las etapas "hacer" y "verificar" se utilice en las etapas de "actuar" y "planificar". En teoría, esto es cíclico, sin embargo, es más una espiral ascendente a medida que ese implementa lo aprendido.

AUDITORÍA/ MENTALIDAD BASADA EN RIESGOS

Las auditorías son un enfoque de proceso sistemático, basado en evidencias, para la evaluación de su SGCN. Se llevan a cabo interna y externamente para verificar la eficacia del sistema de gestión. Las auditorías son un ejemplo brillante de cómo se adopta la mentalidad basada en riesgos dentro de la gestión de la continuidad de negocio.

Auditoría de 1ª parte: auditoría interna

Las auditorías internas son una oportunidad para aprender. Proporcionan tiempo para concentrarse en un proceso o departamento en particular con el fin de evaluar su desempeño. El propósito de una auditoría interna es garantizar el cumplimiento de las políticas, los procedimientos y los procesos determinados por la organización, y confirmar el cumplimiento de los requisitos de la norma ISO 22301.

Planificación de la auditoría

Diseñar un programa de auditoría puede parecer un ejercicio complicado. Dependiendo de la escala y complejidad de sus operaciones, puede programar auditorías internas mensiuales o anuales. Hay más detalles sobre esto en la sección 9: evaluación del desempeño.

Mentalidad basada en riesgos

La mejor manera de considerar la frecuencia de las auditorías es observar los riesgos involucrados en el proceso o área de negocio a auditar. Cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de salir mal o porque las consecuencias serían graves si saliera mal, debería ser auditado con más frecuencia que un proceso de bajo riesgo.

La forma de evalución del riesgo depende totalmente de usted. La ISO 22301 no dicta ningún método particular de evaluación o gestión de riesgos.

2ª parte: auditoría externa

Las auditorías de 2ª parte suelen ser realizadas por clientes o por terceros en su nombre, o puede realizarlas a sus proveedores externos. Las auditorías de terceros también pueden ser realizadas por reguladores o cualquier otra parte externa que tenga un interés formal en una organización.

Es posible que tenga poco control sobre el momento y la frecuencia de estas auditorías, sin embargo, el establecimiento de su propio SGCN garantizará que esté bien preparado.

3ª parte: auditoría de certificación

Las auditorías de 3ª parte las llevan a cabo organismos externos, normalmente organismos de certificación acreditados por UKAS como NQA.
El organismo de certificación evaluará la conformidad con lan orma ISO 22301:2019. Esto implica que un representante del organismo de certificación visite la organización y evalúe el sistema relevante y sus procesos. Mantener la certificación también implica reevaluaciones periódicas.

La certificación demuestra a los clientes que tiene un compromiso con la calidad.

La certificación garantiza:

- Evaluación periódica para controlar y mejorar continuamente los procesos.
- Credibilidad de que el sistema pueda lograr los resultados previstos.
- Reducir el riesgo e incertidumbre y aumentar las oportunidades de mercado.
- Coherencia en los productos para satisfacer las expectativas de las partes interesadas.

AUDITORÍA/ MENTALIDAD BASADA EN PROCESOS

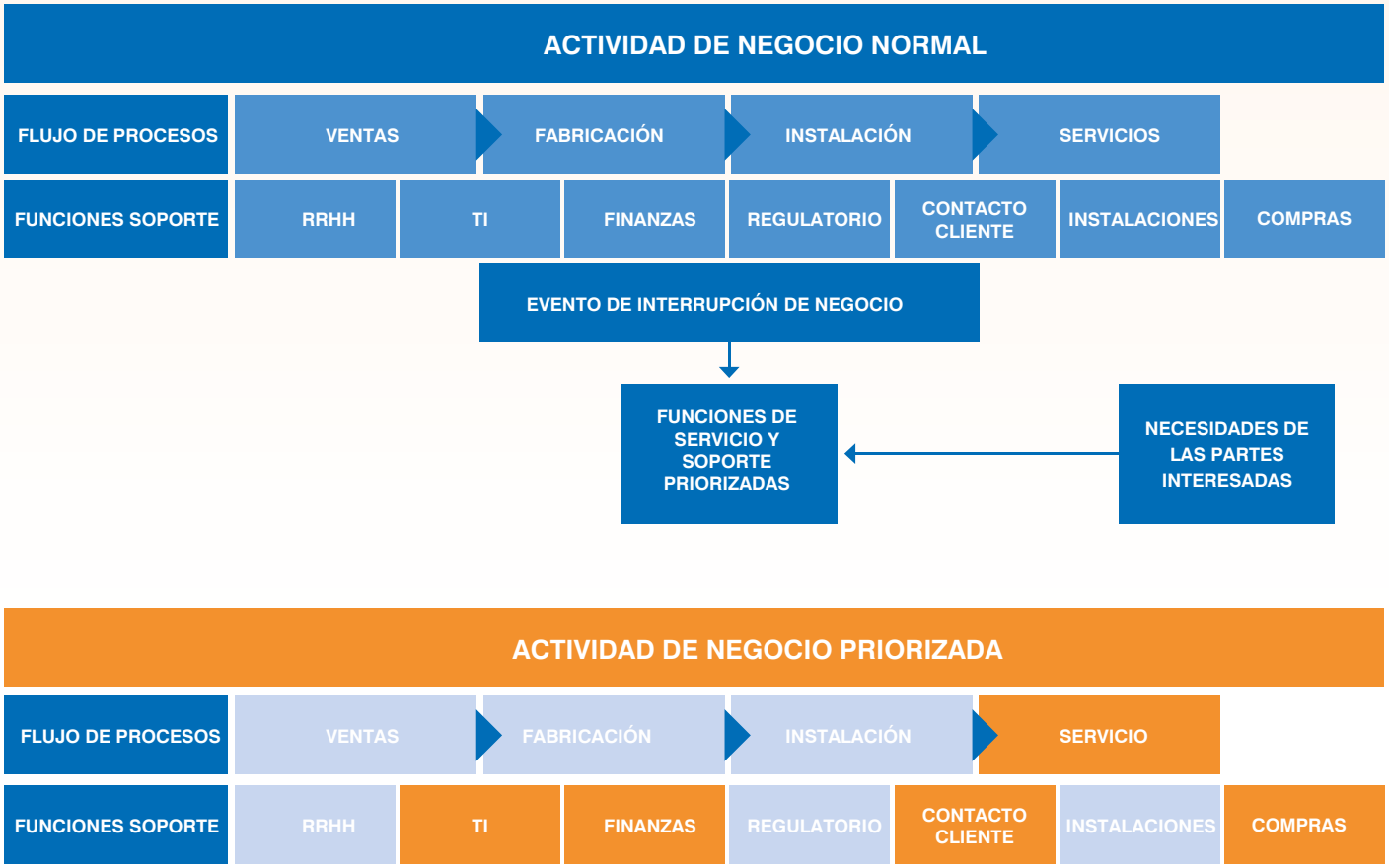
Un proceso es la transformación de insumos en productos, que tiene lugar como una serie de pasos o actividades que dan como resultado los objetivos planificados. A menudo, la salida de un proceso se convierte en una entrada para otro proceso posterior. Muy pocos procesos operan de forma independiente.

El pensamiento basado en procesos es fundamental para la planificación de la continuidad de negocios. Para lograr los objetivos de continuidad de negocio, una organización debe crear planes de continuidad de negocio que se basarán en procesos, abarcando múltiples procesos y funciones organizacionales.

En la práctica, esto significa que un sistema de continuidad de negocio debe considerarse el proceso de un extremo a otro a través de la organización e incorporar funciones de soporte relevantes para lograr sus objetivos.

Es poco probable que un SGCN que sea aplicable a un solo departamento logre objetivos de continuidad válidos.

El siguiente diagrama ilustra cómo una organización podría considerar priorizar los objetivos de su comunidad empresarial a través de su estrategia de continuidad de negocio. En el siguiente ejemplo, una organización que proporciona equipos de atención médica críticos prioriza su actividad de servicio y funciones de soporte clave después de un evento disruptivo importante.

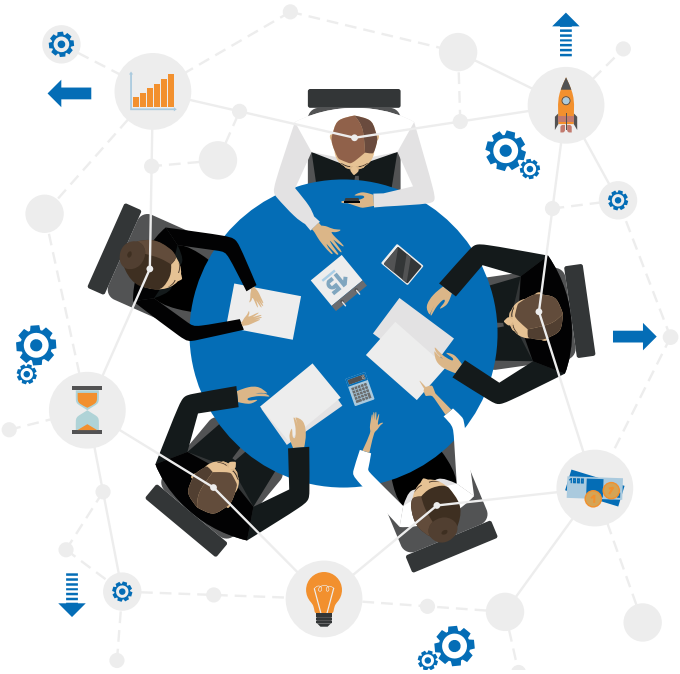


ANEXO SL

Uno de los principales cambios introducidos en la ISO 22301:2019 fue la adopción del Anexo SL para la estructura de cláusulas de la norma. Los redactores de normas utilizaron el Anexo SL (anteriormente conocido como Guía ISO 83) de la ISO para proporcionar una estructura central común para las normas de sistema de gestión.

La ISO 22301 (sistema de gestión de la continuidad de negocio) adoptó esta estructura durante su revisión de 2019. La ISO 27001 (sistema de gestión de seguridad de la información) también adoptó esta estructura durante su revisión de 2013, así como ISO 14001 (sistema de gestión ambiental) que adoptó esta estructura durante su revisión de 2015. La ISO 45001 (sistema de gestión de seguridad y salud) recientemente publicada también sigue esta misma estructura.

Antes de la adopción del Anexo SL, existían muchas diferencias entre la estructura de las cláusulas, los requisitos, términos y definiciones utilizados en las distintas normas de sistemas de gestión. Esto dificultaba la integración de múltiples sistemas de gestiçon dentro de una misma empresa: Medioambiente, Calidad, Seguridad y Salud en el Trabajo y Seguridad de la Información se encuentran entre los más comunes.



Estructura de alto nivel

El anexo SL está formado por 10 cláusulas:

1. Alcance
2. Referencias normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejora

De estas cláusulas, los términos comunes y las definiciones básicas no se pueden cambiar. Los requisitos no se pueden eliminar ni modificar, sin embargo, se pueden agregar requisitos y recomendaciones específicos de la disciplina.

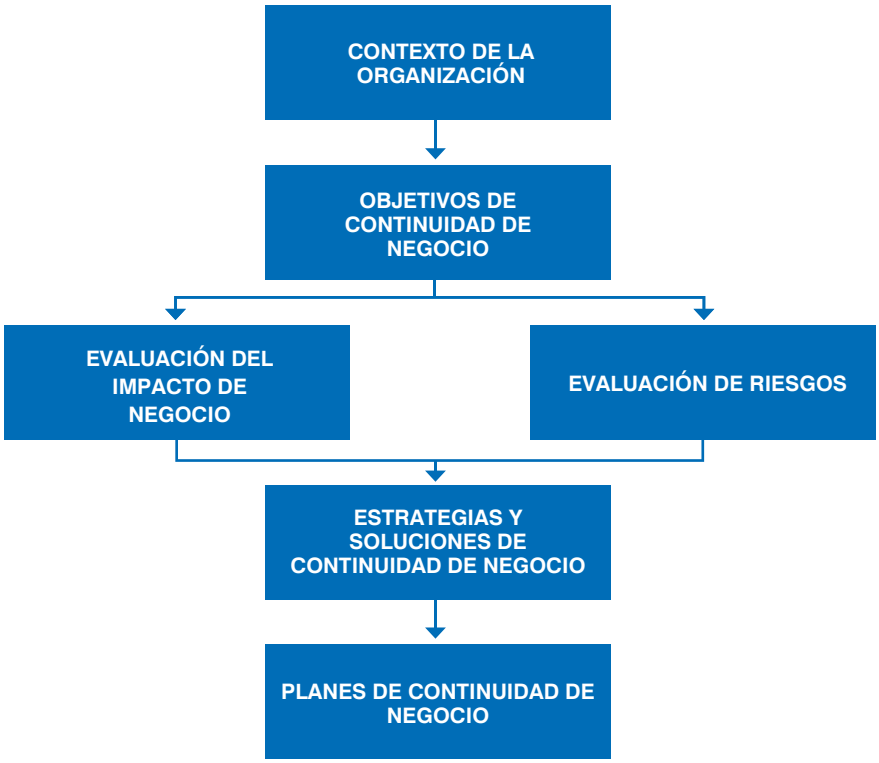
Todos los sistemas de gestión requieren una consideración del contexto de la organización. Un conjunto de objetivos relevantes para la disciplina, en este caso de calidad, y alineados con la dirección estratégica de la organización; una política documentada para respaldar el sistema de gestión y sus objetivos; auditorías internas y revisión por la dirección. Cuando existen múltiples sistemas de gestión, muchos de estos elementos se pueden combinar para abordar más de una norma.

LAS 10 CLÁUSULAS DE ISO 22301:2019

ISO 22301 is made up of 10 sections, known as clauses.

Como ocurre con la mayoría de normas de sistemas de gestión ISO, los requisitos de la ISO 22301 que deben cumplirse se especifican en las cláusulas 4.0 - 10.0. Al igual que en ISO 27001, la organización debe cumplir con todos los requisitos de las Cláusulas 4.0 - 10.0; no pueden declarar que una o más cláusulas no son aplicables.

El diagrama de flujo de la derecha proporciona un ilustrativo de los conceptos de la norma:



CLÁUSULA 1: ALCANCE

La sección del alcance de la ISO 22301 establece:

- El propósito de la norma.
- Los tipos de organizaciones a las que es de aplicación.
- tLas secciones de la norma (llamadas cláusulas) que contienen requisitos que una organización debe cumplir para que la organización sea "conforme" con la norma y reciba la certificación.

ISO 22301 está diseñado para ser aplicable a cualquier tipo de organización, independientemente del tamaño, complejidad, sector, propósito o madurez, cualquier organización puede implementar y mantener un SGCN que cumpla con la ISO 22301.

CLÁUSULA 2: **REFERENCIAS NORMATIVAS**

En las normas ISO, la sección de referencias normativas enumera cualquier otra norma que contengan información adicional relevante para determinar si una organización cumple o no con la norma en cuestión. En la ISO 22301 solo se enumera un documento: ISO 22300, Seguridad y resiliencia - Vocabulario.

Algunos de los términos utilizados o los requisitos detallados en ISO 22301 se explican con más detalle en ISO 22300. La referencia a ISO 22300 es muy útil para ayudarlo a comprender mejor un requisito o identificar la mejor manera de cumplir con el mismo.

Consejo: los auditores externos esperarán que haya tenido en cuenta la información contenida en la ISO 22300 en el desarrollo e implementación de su SGCN.

CLÁUSULA 3: TÉRMINOS Y DEFINICIONES

Hay 31 términos y definiciones en ISO 22301 y se hace referencia a la versión más actual de LA ISO 22300: Seguridad y Resiliencia - Vocabulario. La versión actual de este documento contiene 277 definiciones de términos que se utilizan en ISO 22301.

Además de los términos de la sección "Principios clave y terminología" anterior, otros términos importantes en ISO 22301 son:

Continuidad de negocio

– Capacidad de una organización para continuar la entrega de productos o servicios a niveles predefinidos y aceptables tras una interrupción.

Gestión de la continuidad de negocio

– Proceso de gestión integral que identifica las potenciales amenzadas a una organización y el impacto que pueden causar en las operaciones comerciales, y proporciona un marco para desarrollar la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarda los intereses de las partes interesadas, reputación, marca y actividades de creación de valor.

Plan de continuidad de negocios

– Procedimientos documentados que guían a una organización para responder, recuperarse, reanudar y restablecerse a un nivel de operación predefinido tras una interrupción.

Análisis de impacto al negocio (BIA)

– Proceso de análisis de actividades y el efecto que una interrupción de negocio puede tener sobre ellas.

Equipo de gestión de crisis

– Grupo de funcionalidad individual responsable de dirigir el desarrollo y ejecución del plan de respuesta y continuidad operativa, declarando una interrupción operativa o situación de de emergencia, y proporcionando dirección durante el proceso de recuperación, tanto antes como después del incidente.

Interrupción

– Evento anticipado (por ejemplo, una huelga laboral o un huracán) o no anticipado (por ejemplo, un apagón o un terremoto), que causa una desviación negativa no planificada en la entrega esperada de productos o servicios de acuerdo con los objetivos de una organización.

Invocación

– Acto de declarar que los acuerdos de continuidad de negocio de una organización deben ponerse en vigencia para continuar la entrega de productos o servicios clave.

Periodo máximo tolerable de interrupción (MTPD)

– Tiempo para que los impactos adversos, que pueden surgir como resultado de no proporcionar un producto/servicio o realizar una actividad, se vuelvan inaceptables.

Requisitos mínimos de continuidad de negocio(MBCO)

– Nivel mínimo de servicios y /o productos aceptable para una organización con el fin de lograr sus objetivos comerciales durante una interrupción.

Objetivo de punto de recuperación (RPO)

– Punto en el que la información utilizada por una actividad puede restaurarse para permitir que la actividad se reanude.

Objetivo de tiempo de recuperación (RTO)

– Período de tiempo tras un incidente dentro del cual se reanuda un producto, servicio o actividad o se recuperan recursos.

Al redatctar la documentación de su SGCN, no es necesario que utilice estos términos exactos. Sin embargo, definir los términos que ha utilizado ayuda a aclarar el significado y la intención de los mismos. Puede resultar útil proporcionar un glosario dentro de la documentación del sistema.

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

El propósito del SGCN es permitir que una organización responda de manera efectiva a un incidente perturbador y continuar la entrega de productos y servicios clave a un nivel predefinido, hasta la reanudación de las operaciones normales.

Contexto interno

A continuación se muestran ejemplos de las áreas que deben tenerse en cuenta al evaluar los problemas internos que pueden influir en el SGCN:

- Madurez: ¿es usted una start-up ágil con un lienzo en blanco para trabajar o una institución de más de 30 años con procesos bien establecidos y planes de contingencia?
- Cultura organizacional: ¿Es flexible su empresa sobre cómo, cuándo y dónde trabaja la gente, o está muy regulada en este sentido?
- Dependencias: ¿Cuáles son las dependencias internas necesarias para responder eficazmente al incidente disruptivo?

- Gestión: ¿existen canales y procesos de comunicación claros desde los tomadores de decisiones hacia el resto de la organización?
- Tamaño de los recursos: ¿Trabaja con una cantidad limitada de recursos, personal y equipo?
- Madurez de los recursos: ¿Está el personal bien informado, capacitado y son de confianza o no tienen experiencia y cambina constantemente?

- Coherencia: ¿cuenta con procesos uniformes en toda la organización o una multitud de prácticas operativas diferentes con poca coherencia?
- Equipo: ¿necesita equipo especializado?

Contexto externo

Los siguientes son ejemplos de las áreas que se pueden considerar al evaluar los problemas externos que pueden influir en el SGCN:

- Propietario: ¿necesita aprobación para mejorar la seguridad física?
- Proveedores: ¿sus proveedores pueden proporcionarle a tiempo?
- Reguladores/organismos de aplicación: ¿existen requisitos reglamentarios o estatutarios que deba considerar al desarrollar su SGCN? ¿Necesita informarles que ha desarrollado un plan de continuidad de negocios?
- Económico/político: ¿las fluctuaciones monetarias afectan a su organización?
- Dependencias: ¿Cuáles son las dependencias externas que necesita para responder eficazmente al incidente disruptivo (servicios de TI, suministros, energía, equipos)?
- Consideraciones medioambientales: ¿existen problemas medioambientales que puedan afectar a su SGCN?
- Clientes: ¿qué impacto tendrá el SGCNen sus clientes? ¿necesita informarles?

- Accionistas: ¿Se preocupan estos por la capacidad de su organización para responder a un incidente disruptivo?

Partes interesadas

Es cualquier persona que pueda verse afectada por su SGCN. Se determinarán a través de un análisis exhaustivo de los problemas internos y externos. Es probable que incluyan accionistas, propietarios, reguladores, clientes, empleados, proveedores y pueden extenderse al público en general y al medio ambiente, según la naturaleza de su negocio. No es necesario que intente comprender o satisfacer todas sus necesidades, pero sí debe determinar cuáles de sus necesidades y expectativas relevantes para su SGCN.

Legal y regulatorio

Identificar y mantenerse actualizado con los requisitos legales y reglamentarios relacionados con la continuidad de sus productos y servicios, actividades y recursos al implementar y mantener su SGCN.

- Documentar: documente su requisito de cumplimiento legal, reglamentario y de otro tipo y su enfoque para cumplir con esos requisitos.

Alcance del sistema de gestión

Para cumplir con ISO 22301, debe documentar el alcance de su SGCN. Los alcances documentados suelen describir:

- Los límites físicos o sedes incluidas (o no incluidas)
- Los grupos de empleados internos y externos incluidos (o no incluidos)
- Los procesos, actividades, productos o servicios internos y externos incluidos (o no incluidos)
- Interfaces clave en los límites del alcance.

Si desea priorizar los recursos mediante el desarrollo de un SGCN que no cubra a toda su organización o sus actividades, debe seleccionar un alcance que se limite a administrar los intereses clave de las partes interesadas con un enfoque pragmático. Esto se puede hacer incluyendo solo sedes activos, procesos, productos y unidades de negocio o departamentos específicos.

Consejo: documente o mantenga un archivo de toda la información recopilada en su análisis del contexto de su organización y las partes interesadas, como:

- Diálogo con un representante de la gerencia de la organización.
- Actas de reuniones o planes de negocios.
- Un documento específico que identifica los problemas internos/externos y las partes interesadas y sus necesidades y expectativas. Ejemplo: un análisis DAFO, un estudio PESTLE o una evaluación de riesgo empresarial de alto nivel.

CLÁUSULA 5: LIDERAZGO

Compromiso con el liderazgo

El liderazgo en este contexto significa participación activa en el establecimiento del SGCN, promoviendo su implementación, destacando su importancia y asegurando que los recursos apropiados estén disponibles.

- Asegurando que la política y objetivos de continuidad del negocio estén establecidos y alineados con la dirección estratégica de la organización.
- Asegurando la integración de los requisitos del SGCN en las prácticas comerciales de la organización.
- Asegurando que se cuente con los recursos adecuados
- Comunicando la importancia de la continuidad del negocio y cumpliendo con los requisitos del SGCN.
- Asegurando que el SGCN logre los resultados previstos
- Dirigiendo y apoyando a las personas para contribuir a la eficacia del SGCN.
- Promoviendo la mejora continua.
- Apoyarndo otros roles gerenciales para demostrar su liderazgo y compromiso.

La ISO 22301 otorga gran importancia al compromiso activo de la gerencia en el SGCN, basado en el supuesto de que su compromiso es crucial para garantizar la implementación, el mantenimiento y la mejora continua eficaz de un SGCN eficaz por parte del grupo de empleados en general.

Política de continuidad de negocio

Parte del liderazgo es establecer y documentar una política de continuidad de negocio alineada con la dirección estratégica de la organización. Los requisitos del SGCN deben integrarse en los procesos comerciales y contar con los recursos adecuados.

La política debe:

- Ser apropiada para el propósito de la organización.
- Proporcionar un marco para establecer objetivos de continuidad.
- iIncluye el compromiso de satisfacer los requisitos aplicables.
- iIncluye el compromiso de mejorar continuamente el SGCN.
- Ser comunicada a la organización.
- Estar disponible para las partes interesadas según corresponda.

La Política de continuidad del negocio puede incluir subpolíticas que cubren procesos y actividades clave que son importantes para la provisión continua de productos y servicios clave en caso de un incidente disruptivo y la recuperación de las operaciones normales. Para demostrar la importancia de la misma, debe ser autorizada por la gerencia.

Consejo: para garantizar que su política de continuidad de negocio esté bien comunicada y disponible para las partes interesadas, es una buena idea:

- Incluirla en paquetes de inducción y presentaciones para nuevos empleados y contratistas.
- Publicarla clave en tablones de anuncios internos, intranets y en el sitio web de su organización.
- Hacer que su cumplimiento y/o soporte sea un requisito contractual para los empleados, contratistas y proveedores críticos.

Roles y responsabilidades

Los roles y responsabilidades para la continuidad del negocio deben establecerse, asignarse y comunicarse dentro de la organización.

Se deben asignar responsabilidades para:

- Asegurarse de que el SGCN cumple con los requisitos de la norma.
- Informar sobre el desempeño del SGCN a la gerencia.

Para que la continuidad del negocio forme parte de las actividades diarias, las responsabilidades de continuidad del negocio y las responsabilidades de todo el personal deben definirse, comprenderse y comunicarse.

Evidenciar el liderazgo al auditor

La gerencia es el grupo de personas que establecen la dirección estratégica de una organización y aprueban las asignaciones de recursos a la organización o área empresarial dentro del alcance del SGCN. Según el tamaño y la estructura de su organización, estas personas pueden ser o no el equipo de gestión del día a día.

Por lo general, un auditor probará el compromiso de liderazgo entrevistando a uno o más miembros de la gerencia y evaluando su nivel de implicación y participación en:

- Evaluación de riesgos y oportunidades.
- Establecimiento y comunicación de políticas.
- Establecimiento y comunicación de objetivos.
- Revisión y comunicación del desempeño del sistema.
- Asignación de recursos, responsabilidades y responsabilidades adecuadas.

SUGERENCIA: antes de su auditoría externa, identifique el miembro de la gerencia que se reunirá con el auditor externo y prepárelo para la entrevista con un resumen de las posibles preguntas que le formularán.

CLÁUSULA 6: PLANIFICACIÓN

Al planificar el SGCN, la organización debe tener en cuenta los riesgos y oportunidades identificados al determinar el contexto de la organización y el alcance del sistema. La organización necesita determinar qué riesgos y oportunidades deben abordarse para:

- **Asegurar que el SGCN puede lograr los resultados previstos.**
- **Prevenir o reducir los efectos no deseados.**
- **Lograr una mejora continua.**

Gestión de riesgos y oportunidades

La organización debe establecer una metodología para evaluar riesgos y oportunidades que impactan en la capacidad del SGCN para lograr los resultados previstos y determinar la acción requerida para abordar el riesgo y las oportunidades.

La organización debe:

- Identificar acciones para abordar riesgos y oportunidades.
- iImplementar las acciones identificar.
- Evaluar la efectividad de estas acciones.

Objetivos de continuidad de negocio (y planificación)

Los objetos de continuidad del negocio deben establecerse en funciones y niveles relevantes dentro de la organización. Los objetivos pueden ser a nivel organizacional o departamental.

Los objetivos deben:

- Ser consistentes con la política de continuidad de negocio.
- Ser medibles.
- Tener en cuenta los requisitos aplicables.
- Estarcomunicados.
- Estra controlados y actualizados según corresponda.

Los objetivos deben comunicarse a las personas relevantes dentro de la organización; ser monitoreados y actualizados según sea necesario.

Consecución de objetivos

La organización debería establecer un plan para lograr sus objetivos; el plan debe tener en cuenta:

- Que debe hacerse.
- Los recursos necesarios.
- Quien es responsable.
- Le fecha de consecución.
- Cómo es evalúan los resultados.

Cambios en el SGCN

Es probable que con el tiempo cambien los procesos, actividades, productos y servicios de la organización. Como resultado, deberá realizar cambios en su SGCN, los cambios deben realizarse de manera planificada y deben tener en cuenta:

- El propósito del cambio y sus posibles consecuencias.
- La integridad del SGCN.
- La disponibilidad de recursos.
- La reasignación de responsabilidades y autoridades.


IDEA
SUCCESS
INCOME
IDEA
Product
MONEY
Business
SUCCESS
IDEA
MONEY

CLÁUSULA 7: SOPORTE

La cláusula 7 se refiere a los recursos. Esto se aplica tanto a personas, infraestructura y medioambiente como a recursos físicos, materiales, herramientas, etc. También hay un enfoque renovado en el conocimiento como un recurso importante dentro de su organización. Al planificar los objetivos de continuidad de negocio, una consideración importante será la capacidad actual y la capacidad de sus recursos, así como los que pueda necesitar de proveedores/socios externos.

Recursos

Para implementar y mantener un SGCN eficaz, la organización necesita identificar y proporcionar los recursos de apoyo necesarios para operarlo, mantenerlo y mejorarlo continuamente.

Dichos recursos deben ser:

- Capaces: si el recurso es equipo o infraestructura.
- competentes: si son personas.
- suficientes: si son suministros.

Competencia

La implementación de un SGCN eficaz depende en gran medida del conocimiento y las habilidades de sus empleados, proveedores y contratistas. Para tener la certeza de contar con una base adecuada de conocimientos y habilidades, debe:

- Definir los conocimientos y las habilidades que se requieren.
- Determinar quién necesita conocimientos y habilidades.
- Verificar que las personas adecuadas tengan los conocimientos y las habilidades adecuadas.

Su auditor esperará que tenga documentos que detallen los requisitos de conocimientos y habilidades. Cuando crea que se cumplen los requisitos, será necesario respaldarlo con registros como certificados de capacitación, de asistencia a cursos o evaluaciones internas de competencia.

Consejo: la mayoría de organizaciones que ya utilizan herramientas como matrices de capacitación/habilidades, o evaluaciones de proveedores pueden satisfacer el requisito de registros de competencia al expandir las áreas cubiertas para incluir la continuidad de negocio.

Toma de conciencia

Además de garantizar la competencia específica del personal clave en relación con la continuidad del negocio, los empleados, proveedores y contratistas deberá conocer los elementos básicos del SGCN. Esto es fundamental para establecer una cultura de apoyo dentro de la organización.

Todo el personal, proveedores y contratistas deben conocer lo siguiente:

- Que tiene un SGCN y la razón.
- Que tiene una política de continuidad de negocio y qué elementos particulares de la misma son relevantes para ellos.
- Cómo pueden contribuir a que su organización responda a una situación adversa y mantenga la continuidad de los productos o servicios en un nivel predefinido.
- Qué políticas, procedimientos son relevantes para ellos y cuáles son las consecuencias de no cumplirlos.

Consejo: la comunicación de esta información normalmente se realiza a través de procesos y documentos existentes, como inducción del personal, contratos de trabajo, charlas, acuerdos con proveedores, reuniones informativas o actualizaciones.

Comunicación

Para permitir que los procesos en su SGCN funcionen de manera efectiva, deberá asegurarse de tener actividades de comunicación bien planificadas y administradas.

Una organización debe establecer:

- Que necesita ser comunicado.
- Cuando necesita ser comunicado.
- A quien necesita ser comunicado.
- Cuales son los procesos de comunicación.
- Quién es responsable de la comunicación.

Consejo: si sus requisitos de comunicación están bien definidos en sus procesos, políticas y procedimientos, no necesita hacer nada más para satisfacer este requisito. Si no es así, debería considerar la posibilidad de documentar sus actividades de comunicación clave en forma de una tabla o procedimiento que incluya los títulos detallados anteriormente. Recuerde, el contenido de estos documentos también debe comunicarse.

Información documentada

Para ser de utilidad, la información documentada que utiliza para implementar, mantener y mejorar su SGCN debe:

- Ser precisa.
- ser clara, inequívoca y comprensible para las personas que lo usan con regularidad u ocasionalmente.
- Respaldar el cumplimiento de los requisitos legales y gestionar riesgos y problemas que afectan la capacidad del SGCN para lograr los resultados previstos.

Para que su información documentada cumpla con estos requisitos, deberá contar con procesos para garantizar que:

- La información documentada es revisada por personas adecuadas antes de que se publique.
- La información documentada está disponible donde y cuando se requiere y es adecuada para su uso.
- El acceso a la información documentada está controlado de manera que no pueda ser modificada, corrompida, eliminada o accedida por personas no autorizadas.
- La información se elimina de forma segura o se devuelve a su propietario cuando se solicita.
- Puede realizar un seguimiento de los cambios en la información para garantizar que el proceso esté bajo control.

La fuente de su información documentada puede ser interna o externa, por lo que sus procesos de control deben administrar la información documentada de ambas fuentes.

Consejo: las organizaciones que tienen un buen control documental suelen presentar los siguientes aspectos:

- Persona o equipo responsable de garantizar que los documentos nuevos/modificados se revisen antes de su emisión, se almacenen en la ubicación correcta, se retiren de la circulación cuando se reemplacen y que se mantenga un registro de cambios.
- Un sistema de gestión de documentos electrónicos que contiene controles y flujos de trabajo automáticos.
- Copias de datos electrónicos y procesos de archivado/almacenamiento de archivos impresos robustos.
- Fuerte conciencia de los empleados sobre los requisitos de control de documentos, mantenimiento de registros y acceso/retención de información.

CLÁUSULA 8: OPERACIÓN

Completadas las actividades de planificación y evaluación de riesgos requeridas por la norma, ahora pasamos a la etapa de implementación y operación. Aquí es donde se implementan y controlan los procesos y acciones identificados para abordar los riesgos y oportunidades.

Las siguientes prácticas son cruciales para implementar procesos efectivos:

1. Los procesos se crean adaptando o formalizando las actividad de negocio normal de una organización.
2. Identificación sistemática de los riesgos de continuidad de negocio para cada producto y servicio.
3. Definición y comunicación clara del conjunto de actividades necesarias para gestionar los riesgos asociados a la continuidad del negocio.
4. Asignación clara de responsabilidades para la realización de actividades relacionadas.
5. Asignación adecuada de recursos para asegurar que las actividades relacionadas puedan llevarse a cabo cuando sea necesario.
6. Evaluación de rutina de la coherencia con la que se sigue cada proceso y su eficacia en la gestión de los riesgos de continuidad del negocio.

Consejo: Designe a una persona como responsable de garantizar que se cumplan los pasos 2 a 6 para cada proceso. Este individuo es conocido como propietario del proceso.

Análisis del impacto de negocio y evaluación de riesgos

Se requiere que una organización implemente y mantenga un proceso para analizar el impacto de negocio y evaluar el riesgo de interrupción de sus actividades clave. Los resultados del análisis del impacto de negocio y las evaluaciones de riesgos permitirán a una organización determinar la estrategia y la solución adecuadas necesarias para responder a un incidente disruptivo.

Análisis del impacto de negocio

El propósito de realizar un análisis de impacto empresarial es permitir que una organización identifique sus requisitos y prioridades de continuidad de negocio. El proceso para realizar un análisis de impacto de negocio deberá:

- Definir los tipos de impacto y los criterios relevantes para el contexto de la organización.
- Identificar y priorizar las actividades clave y los productos y servicios necesarios para lograrlas.
- Evaluar los impactos desde la interrupción hasta las actividades.
- Identificar el momento en el que la no reanudación de estas actividades tendría un impacto perjudicial en la organización (MTPD).
- Identificar el momento en que la reanudación de estas actividades se reanudará a un nivel aceptable (RTO).
- identificar los recursos para apoyar las actividades priorizadas.
- Determinar las dependencias internas y externas necesarias para respaldar las actividades prioritarias.

Evaluación de riesgos

El proceso de evaluación de riesgos permitirá a la organización determinar la probabilidad de ocurrencia de incidente. Tras identificar las acciones necesarias para reducir la probabilidad y el impacto en las actividades priorizadas de la organización en caso de un incidente disruptivo. Las evaluaciones de riesgos deben realizarse a intervalos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera.

El proceso de evaluación de riesgos deberá:

- Identificar los riesgos para las actividades priorizadas de la organización y sus recursos requeridos.
- Analizar y evaluar el riesgo identificado.
- Determinar los riesgos que requieren tratamiento.

Estrategia de continuidad de negocio y soluciones

Los resultados del análisis de impacto de negocio y la evaluación de riesgos se utilizarán para determinar la estrategia correcta de continuidad de negocio e identificar los recursos necesarios para responder y gestionar el incidente de continuidad hasta que se reanuden las operaciones normales.

Selección de estrategias y soluciones:

La selección de la estrategia y las soluciones de continuidad del negocio de una organización se basará en:

- La capacidad de cumplir con los requisitos para continuar y recuperar actividades priorizadas en una capacidad predeterminada y en un plazo acordado.
- Reducir la probabilidad y el período de interrupción.
- Los recursos necesarios.
- La tolerancia del riesgo de la organización.
- Costes y beneficios.

Requisitos de recursos

Al determinar el recurso requerido para la implementación de la solución de continuidad del negocio, la organización debe considerar los recursos internos y externos requeridos.

Los recursos mínimos incluyen:

- Personal.
- información y datos.
- infraestructura e instalaciones de soporte.
- Equipamiento y bienes.
- Sistemas de TI y telecomunicaciones.
- Transporte y logística.
- Finanzas.
- Socios y proveedores.

Plan y procedimientos de continuidad de negocio

Basado en el resultado de las estrategias y soluciones de continuidad de negocio seleccionadas, se requiere que la organización establezca una estructura de respuesta e implemente planes y procedimientos para administrar la organización durante un incidente disruptivo que requiera la activación de soluciones de continuidad del negocio.

Los procedimientos deberán:

- Identificar los pasos tomados durante una interrupción.
- Adaptarse a los cambios en las condiciones internas y externas como resultado de la interrupción.
- Centrarse en el impacto de incidentes que causen interrupción.
- Minimizar el impacto de la interrupción.
- Asignar roles y responsabilidades para las tareas.

Estructura de la respuesta

La estructura de respuesta constará de uno o más equipos de gestión de crisis responsables de responder y gestionar las interrupciones. Los roles y responsabilidades de cada equipo deben estar claramente definidos, deben ser competentes para evaluar el impacto de la interrupción e implementar la respuesta apropiada de continuidad de negocio. La estructura de la respuesta debe incluir procedimientos para comunicarse con partes interesadas, autoridades y medios de comunicación.

Planes de continuidad de negocio

Se deben desarrollar y mantener planes y procedimientos documentados de continuidad de negocio que brinden orientación e información para permitir que los equipos respondan a un incidente perturbador y la recuperación de las operaciones normales. Los planes deben estar disponibles donde y cuando sea necesario.

Los planes de continuidad de negocio deben contener:

- Detalles de acciones que tomará cada equipo para continuar o recuperar actividades priorizadas, monitorear el impacto de la interrupción y la respuesta de la organización
- Referencia a los umbrales y procesos predefinidos para activar la respuesta,
- Procedimientos para permitir la entrega de productos y servicios a una capacidad acordada.
- Detalles para gestionar las consecuencias inmediatas de una interrupción teniendo en cuenta el bienestar de las personas, la prevención de una mayor interrupción de las actividades priorizadas y el impacto en el medio ambiente.

Cada plan deberá:

- Dar el propósito, alcance y objetivos
- Los roles y responsabilidades del equipo que implementará el plan.
- Identificar acciones para implementar las soluciones.
- Contener la información necesaria para activar, operar, coordinar y comunicar las acciones del equipo.
- Identificar las dependencias internas y externas necesarias.
- Identificar los recursos necesarios.
- Incluir requisitos de informes.
- Un proceso de retirada.

Recuperación

La organización debe tener procesos documentados para volver a la normalidad tras un incidente de continuidad del negocio.

Programa de ejercicios

Para garantizar lque las estrategias, soluciones y planes de continuidad de negocio sigan siendo válidos, se requiere que la organización establezca un programa de ejercicios para probar su eficacia La organización no necesita probar la totalidad de sus acuerdos de continuidad de negocio durante cada ejercicio.

Dichos ejercicios deben:

- Ser coherente con sus objetivos de continuidad empresarial.
- Basarse en escenarios apropiados con metas y objetivos claramente definidos.
- Desarrollar el trabajo en equipo y la competencia de los equipos de continuidad del negocio y sus miembros.
- Validar estrategia, solución y plan de continuidad del negocio.
- Producir informes posteriores al ejercicio que contengan resultados, recomendaciones y acciones de mejora.
- Debe realizarse a intervalos planificados o cuando se produzcan cambios significativos dentro de la organización o el contexto en el que opera.

Evaluación de la documentación y capacidades de continuidad de negocio

La organización debe evaluar la idoneidad y eficacia de su análisis de impacto de negocio, evaluación de riesgos, estrategias, soluciones, planes y procedimientos a intervalos planificados, después de un incidente o interrupción y cuando se produzcan cambios significativos.

CLÁUSULA 9: EVALUACIÓN DEL DESEMPEÑO

Seguimiento, medición, análisis y evaluación

La organización necesita evaluar el desempeño y la eficacia de l SGCN para asegurar que puede lograr los resultados previstos. Necesita determinar qué seguir y medir, los métodos de monitoreo y medición y cómo se evaluarán los resultados. Las acciones de seguimiento y medición deben ser planificadas, el personal que realiza la actividad de seguimiento y medición debe ser identificado y seleccionado teniendo en cuenta la competencia y la imparcialidad. Se debe conservar la evidencia apropiada de la actividad de seguimiento y medición y los resultados de la actividad de la misma.

Auditoría interna

El propósito de las auditorías internas es confirmar que el SGCN se ha implementado de manera efectiva e identificar cualquier debilidad y oportunidades de mejora.

Las auditorías internas deben comprobar:

- Si el SGCN satisface las necesidades de la organización.
- Si cumple con la norma ISO 22301: 2019.
- La consistencia de aplicación de procesos y procedimientos.
- si los procesos y procedimientos logran los resultados esperados.

Programa de auditorías internas

Una organización debe realizar auditorías internas a intervalos planificados. El programa de auditoría deberá:

- Considerar la importancia de los procesos en cuestión y los resultados de auditorías anteriores.
- Definir los criterios y el alcance de cada auditoría.
- Seleccionar auditores y realizar auditorías para garantizar la objetividad e imparcialidad del proceso de auditoría.
- Asegurar que los resultados de la auditoría se informan a la gerencia.
- Retener evidencia documentada de la implementación del programa de auditoría y los resultados de la auditoría.
- Asegurar que se tomen sin demora las acciones correctivas necesarias para abordar las no conformidades y sus causas.

Revisión por la dirección

La gerencia debe revisar el SGCN de la organización a intervalos planificados para evaluar su adecuación, idoneidad y eficacia para satisfacer las necesidades de la organización.

Las entradas y salidas de las reuniones de revisión por la dirección deben cumplir con los requisitos de la cláusula 9.3 de la norma. La salida debe incluir decisiones relacionadas con oportunidades de mejora continua y cualquier cambio necesario para mejorar la eficiencia y eficacia del SGCN.

La organización debe retener información documentada como evidencia de los resultados de las revisiones por la dirección y comunicar los resultados a las partes interesadas relevantes.

CLÁUSULA 10: MEJORA

El objetivo principal de la implementación de un SGCN es garantizar que la organización pueda responder a un incidente disruptivo de manera oportuna y continuar entregando sus productos y servicios clave a un nivel predefinido hasta el retorno a la normalidad operativa.

No conformidad y acción correctiva

Las organizaciones deben determinar oportunidades de mejora e implementar acciones para lograr los resultados previstos de l SGCN. Las organizaciones deben reaccionar ante las no conformidades y tomar medidas para controlar y corregir las no conformidades y hacer frente a las consecuencias.

Análisis de causa raíz

La organización investigará la no conformidad para:

- Establecer si la no conformidad existe en otro lugar.
- Identificar la causa raíz de la no conformidad.
- Identificar cualquier acción correctiva necesaria para evitar la recurrencia de la no conformidad.
- Identificar cualquier cambio requerido en el SGCN.

Cualquier acción correctiva identificada para abordar las no conformidades debe implementarse sin demoras indebida. La acción correctiva implementada se revisará para determinar su efectividad.

SACAR EL MÁXIMO DE SU SISTEMA DE GESTIÓN

Consejos para una implantación efectiva del SGCN:

1. Pregúntese "¿Por qué?". Asegúrese de que las razones para implementar el SGCN sean claras y estén alineadas con su dirección estratégica; de lo contrario, corre el riesgo de no obtener la aceptación de la gerencia.

2. A continuación, considere "¿Para qué?". Implementar y mantener un SGCN requiere un compromiso significativo, así que asegúrese de que su alcance sea lo suficientemente amplio para cubrir la información crítica, pero que no sea tan amplio como para no tener recursos para implementarlo y mantenerlo.

3. Involucre a todas sus partes interesadas clave. Gerencia para el contexto, requisitos, política y establecimiento de objetivos; gerentes y empleados con valiosos conocimientos para evaluación de riesgos, diseño de procesos y redacción de procedimientos.

4. Comuníquese durante todo el proceso con sus partes interesadas. Hágales saber lo que está haciendo, por qué lo hace, cómo planea hacerlo y cuál será su participación. Proporcione actualizaciones sobre el progreso.

5. Solicite ayuda externa donde la necesite. No falle por falta de habilidades o conocimientos técnicos internos. La gestión de riesgos a menudo requiere conocimientos especializados. Asegúrese de verificar las credenciales de un tercero antes de contratarlo.

6. Mantenga procesos y documentación de respaldo simples. Puede desarrollarlos más adelante si es necesario.

7. Diseñe e implemente reglas que pueda seguir en la práctica. No cometa el error de documentar una regla demasiado elaborada que nadie puede seguir. Es mejor aceptar un riesgo y seguir buscando formas de gestionarlo.

8. Recuerde a sus proveedores, dado que algunos lo ayudarán a mejorar su SGCN, otros aumentarán su riesgo. Debe asegurarse de que los proveedores de alto riesgo cuenten con controles apropiados. Si no es así, busque alternativas.

9. Formación y más formación. Es probable que la continuidad de negocio sea un concepto nuevo para la mayoría de sus empleados. Las personas pueden necesitar cambiar hábitos arraigados. Es poco probable que una sola sesión de sensibilización sea suficiente.

10. Recuerde asignar recursos suficientes para probar sus controles de forma rutinaria. Las amenazas a las que se enfrenta su organización cambiarán constantemente y debe probar si es capaz de responder a dichas amenazas.

PASOS TRAS LA IMPLANTACIÓN

1 FORMACIÓN DE CONCIENCIACIÓN

- Su organización debe crear conciencia sobre varios estándares cubiertos por el SGCN.
- Debe realizar reuniones de capacitación separadas para la alta gerencia, la gerencia media y la gerencia de nivel junior, lo que ayudará a crear un entorno motivador, listo para la implementación.

2 POLÍTICA Y OBJETIVOS

- Su organización debe desarrollar una Política de continuidad de negocio/integrada y objetivos relevantes para ayudar a cumplir con los requisitos.
- Al trabajar con la gerencia, su empresa debe realizar talleres con todos los niveles del personal de administración para delinear los objetivos integrados.

3 ANÁLISIS DE DEFICIENCIAS INTERNO

- Su organización debe identificar y comparar el nivel de cumplimiento de los sistemas existentes con los requisitos de los estándares de su nuevo SGCN.
- Todo el personal relevante debe comprender las operaciones de la organización y desarrollar un mapa de procesos para las actividades dentro del negocio.

4 DOCUMENTACIÓN/PROCESO DE DISEÑO

- La organización debería crear documentación de los procesos de acuerdo con los requisitos de las normas pertinentes.
- Debe redactar e implementar un manual de procedimientos funcionales, instrucciones de trabajo, procedimientos del sistema y proporcionar los términos asociados.

5 DOCUMENTACIÓN/PROCESO DE IMPLANTACIÓN

- Los procesos/documentos del paso 4 deben implementarse en toda la organización cubriendo todos los departamentos y actividades.
- La organización debe realizar un taller sobre la implementación según corresponda para los requisitos de la norma ISO.

6 AUDITORÍA INTERNA

- Un sistema de auditoría interna robusto para la organización es esencial. Se recomienda la formación de auditor interno y NQA puede brindar dicha formación para varias normas.
- Es importante implementar acciones correctivas de mejora, en cada uno de los documentos auditados, con el fin de cerrar brechas y asegurar la efectividad del SGCN.

7 ORGANIZAR LA REVISIÓN POR LA DIRECCIÓN DEL SISTEMA

- La gerencia debe revisar varios aspectos comerciales oficiales de la organización, que son relevantes para los estándares que se están implantando.
- Revise la política, objetivos, resultados de la auditoría interna, del desempeño del proceso, de quejas/retroalimentación/cumplimiento legal, de la evaluación de riesgos/incidentes y desarrolle un plan de acción después de la reunión, que debe ser documentado.

8 ANÁLISIS DE DEFICIENCIAS DE SISTEMAS IMPLANTADOS

- Se debe realizar un análisis de deficiencias de precertificación formal para evaluar la efectividad y el cumplimiento de la implementación del sistema en la organización.
- Este análisis final de deficiencias preparará a su organización para la auditoría de certificación final.

9 ACCIONES CORRECTIVAS

- La organización debe estar lista para la auditoría de certificación final, siempre que a la auditoría de análisis de deficiencias realizada en el último paso y a todas las no conformidades (NC) se les hayan asignado acciones correctivas.
- Compruebe que todas las NC importantes estén cerradas y que la organización esté lista para la auditoría de certificación final.

10 AUDITORÍA DE CERTIFICACIÓN FINAL

- Una vez completado, se espera que se recomiende a su organización para que se certifique en la norma requerida.
- ¡FELICIDADES!

Authored by: Tony Bevan, NQA UK Auditor