G

Gestión y Calidad

INTE G130:2022/Cor 1:2023

Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro- Requisitos y orientación para su uso.

Correspondencia: Esta norma nacional no es equivalente (NEQ) con ninguna norma internacional, por no existir referencia alguna al momento de su elaboración.

Miembros de

Fecha: 2022-12-29
Primera Edición
Secretaría: INTECO
Editada e impresa por ©INTECO

ICS 03.100.01

AVISOS IMPORTANTES SOBRE ESTE DOCUMENTO

Aviso y descargo de responsabilidad concerniente al uso de documentos INTECO

Las normas, los documentos normativos y otros instrumentos documentales de la Dirección de Normalización de INTECO, entre ellos el presente, son elaborados a través de un proceso de desarrollo de normas que se llevan a cabo bajo los principios de transparencia, apertura, imparcialidad, consenso, efectividad, relevancia, coherencia y dimensión del desarrollo, que emanan del Organismo Mundial de Comercio (OMC).

Ese proceso reúne a expertos voluntarios en distintas materias, integrados en comités que llevan el nombre del objeto de cada norma y representan distintas visiones. Forman parte los consumidores, empresarios, el Estado, y otros interesados en la norma, que exponen diferentes puntos de vista e intereses para lograr el consenso de la norma; mientras que la Dirección de Normalización de INTECO coordina el proceso y establece reglas para promover la equidad en el consenso para aprobar cada norma. La Dirección de Normalización de INTECO no forma parte de ningún comité, no vota, ni evalúa o verifica el contenido de ninguna norma, solo facilita el proceso de desarrollo de esta.

Por ello, INTECO no se hace responsable por el contenido de cada norma aprobada en un órgano de estudio, ya que esa responsabilidad recae en los miembros que participaron y la aprobaron pues son los expertos en la materia objeto de la norma.

INTECO no aceptará responsabilidad alguna por la aplicación de una norma, en especial no la acepta sobre daño personal, o sobre las cosas o derechos, u otros de cualquier naturaleza, ya sean especiales, directos o indirectos como consecuencia de la utilización del presente documento. Tampoco por la calidad resultante del producto o servicio al cual aplica.

La Dirección de Normalización de INTECO tampoco garantiza la precisión o que la información aquí publicada esté completa. Al expedir y poner este documento a la disposición del público, la Dirección de Normalización de INTECO no se responsabiliza por la prestación de servicios profesionales o de alguna otra índole a nombre de cualquier otra persona o entidad. Si el interesado no es experto o duda del contenido de la norma, deberá buscar la ayuda de un profesional competente y capacitado para determinar el ejercicio razonable en cualquier circunstancia.

La Dirección de Normalización de INTECO, desde el proceso de desarrollo de normas, no tiene poder, ni responsabilidad, para vigilar o hacer cumplir los contenidos de este documento. Este proceso de desarrollo de normas no certifica, prueba o inspecciona productos, diseños o instalaciones en cumplimiento de ninguna norma. Cualquier certificación u otra declaración de cumplimiento con los requerimientos de este documento es únicamente responsabilidad del Ente Certificador o la persona o entidad que hace la declaración.

Las observaciones a este documento han de dirigirse a:

Instituto de Normas Técnicas de Costa Rica

San Pedro de Montes de Oca

San José, Costa Rica

Tel: +506 2283 4522

info@inteco.org

www.inteco.org

CONTENIDO **PÁGINA**

PRÓLOGO

El Instituto de Normas Técnicas de Costa Rica, INTECO, es el Ente Nacional de Normalización, según la Ley N° 8279 del año 2002. Organización de carácter privado, sin ánimo de lucro, cuya Misión es "desarrollar la normalización del país con el soporte de los servicios de evaluación de la conformidad y productos relacionados a nivel nacional e internacional, con un equipo humano competente, con credibilidad e independencia". 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 ha sido desarrollada en cumplimiento de los requisitos de nivel 1 y nivel 2 del Standards Council of Canada (SCC).

Esta norma INTE G130:2022 fue aprobada por INTECO en la fecha del 2022-12-29.

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 organizaciones que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico Nacional CTN 53 SC 01, Continuidad y resiliencia.

Participante	Organización
Mauricio Solano	Consultor
Carlos Quesada	Sonda
Andrea Guevara	CODISA
Ricardo Morales Jennifer de la O	Banco Central de Costa Rica (BCCR)
Rodolfo Romero Álvaro Montero	Universidad de Costa Rica (UCR)
Ana Morera	Florida Ice and Farm Company (FIFCO)
Massiel Vallejos	BAC Credomatic
Carolina Jiménez	Cooperativa de Productores de Leche Dos Pinos R.L
Randall Villalobos S	Banco Nacional de Costa Rica (BNCR)
Víctor Zúñiga	B-Solutionsgroup
Marco Gámez	Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF)
Stephanie Valverde	Instituto Costarricense de Electricidad (ICE)
Fausto Roldán	Radiográfica Costarricense S.A. (Racsa)
Christopher Calderón Luis Jiménez	Cruz Roja
Cristian Aase	Emergencias médicas
Johnny Hidalgo	Sistema de Emergencias 911
Marco Rosales	Benemérito Cuerpo de Bomberos de Costa Rica
Ramón Araya Carlos Mesén	Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE)
Fernando Calderón	Bureau for Humanitarian Assistance (USAID /BHA)

Participante	Organización
Carlos Mora	Universidad Técnica Nacional (UTN)

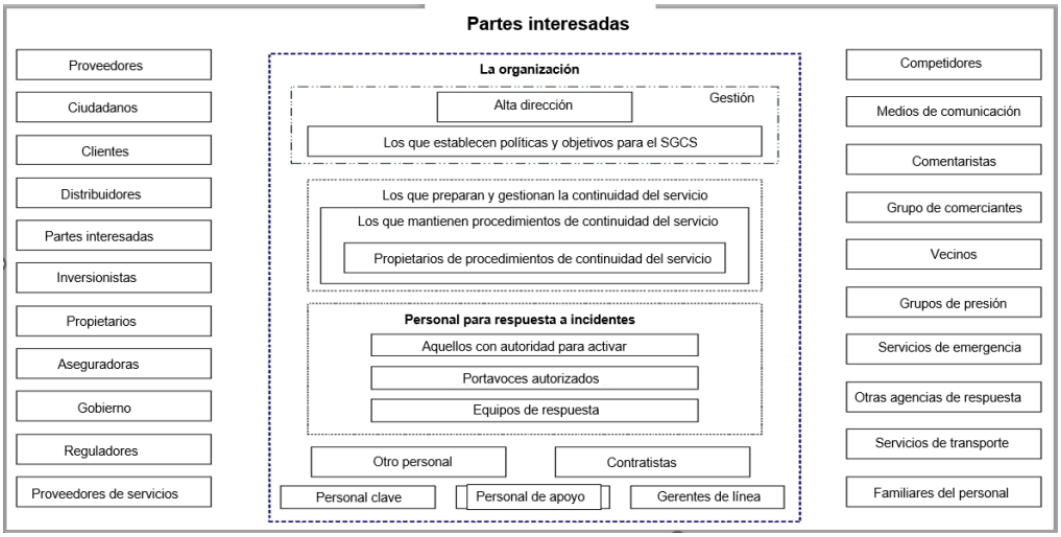
Corrigendo 1

El siguiente corrigendo de la norma nacional INTE G130:2022 fue aprobado por el CTN 53 SC 01 Continuidad y resiliencia en el 2023-02-27.

Página 22, capítulo 4, Figura 2

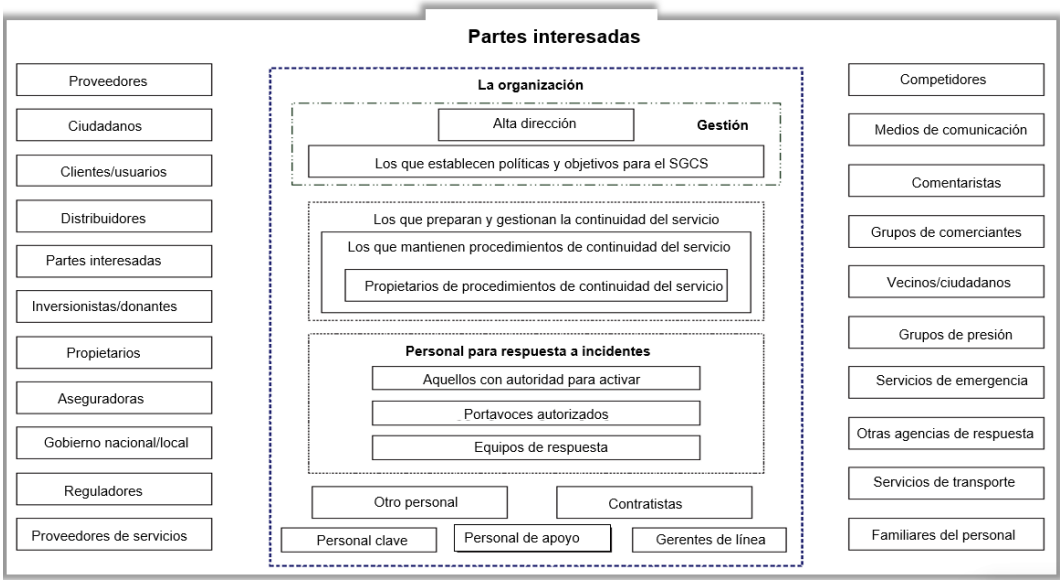
Actual:

Se menciona en la lista izquierda “Clientes” como parte interesada. Además, en la columna derecha se mencionan “Vecinos”.



Modificado:

Se corrige a Clientes/Usuarios y a Vecinos/ciudadanos.



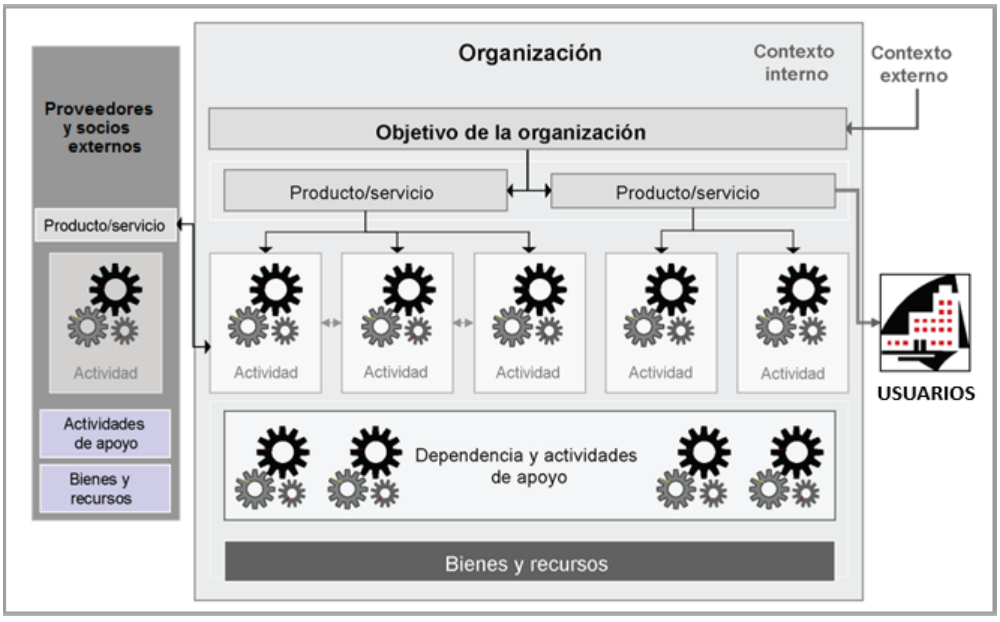
Página 35, capítulo 8, Figura 4

Actual:

Se menciona enn la salidad del proceso a la derecha “Clientes”.

Modificado:

Se corrige a Usuarios.



0 INTRODUCCIÓN

0.1 Generalidades

En este documento se especifican la estructura y los requisitos para la aplicación y el mantenimiento de un sistema de gestión de la continuidad del servicio (SGCS) que permita el desarrollo de las actividades adecuadas a la cantidad y el tipo de impacto que la organización pública o sin fines de lucro pueda o no aceptar tras una disrupción.

Los resultados del mantenimiento de un SGCS están conformados por los requisitos legales, reglamentarios, organizativos, los productos y servicios proporcionados, los procesos empleados, el tamaño y la estructura de la organización y los requisitos de sus partes interesadas.

Un SGCS enfatiza la importancia de:

- comprender las necesidades de la organización pública y sin fines de lucro y la necesidad de establecer políticas y objetivos de continuidad de la actividad;
- operar y mantener procesos, capacidades y estructuras de respuesta para garantizar que la organización sobreviva a las disrupciones;
- supervisar y examinar el desempeño y la eficacia del SGCS;
- la mejora continua basada en medidas cualitativas y cuantitativas.

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

a) política;
b) personas competentes con responsabilidades definidas;
c) procesos de gestión relacionados con la:
    1) política;
    2) planificación;
    3) implementación y operación;
    4) evaluación del desempeño;
    5) revisión de la gestión;
    6) mejora continua;
d) información documentada que apoye el control operacional y permita la evaluación del desempeño.

Se espera que los funcionarios públicos y colaboradores de las organizaciones sin fines de lucro reciban, comprendan y apliquen un plan de desarrollo o un programa de trabajo a corto o mediano plazo con los contenidos del presente documento. Sin embargo, el plan o programa en sí no garantiza que las necesidades y expectativas de las organizaciones sean cubiertas, ya que los procesos necesarios para la implementación efectiva de estos podrían ser deficientes o inexistentes. Para contrarrestar esta condición, el documento se ha desarrollado para ayudar a las organizaciones públicas y sin fines de lucro a establecer las bases y ser una guía para implementar un sistema de gestión de la continuidad del servicio.

0.2 Beneficios de un sistema de gestión de la continuidad del servicio en organizaciones públicas y sin fines de lucro

El propósito de un SGCS es preparar, proporcionar y mantener controles para gestionar la capacidad de una organización pública y sin fines de lucro para seguir funcionando durante las disrupciones.

Para lograr esto, la organización está:

a) desde una perspectiva estratégica:
   1) Apoyando sus objetivos estratégicos;
   2) creando valor público y servicios sin fines de lucro;
   3) protegiendo y mejorando su reputación y credibilidad;
   4) contribuyendo a la resiliencia de la organización;
b) desde una perspectiva financiera:
   1) reduciendo la exposición jurídica y financiera;
   2) reduciendo los costos directos e indirectos de las disrupciones;
c) desde la perspectiva de las partes interesadas:
   1) protegiendo la vida, la propiedad y el ambiente;
   2) considerando las expectativas de las partes interesadas;
   3) proporcionando confianza en la capacidad de la organización para tener éxito;
d) desde la perspectiva de los procesos internos:
   1) mejorando su capacidad para seguir siendo eficaz durante las disrupciones;
   2) demostrando un control proactivo de los riesgos de manera eficaz y eficiente; abordando las vulnerabilidades operacionales.

Como complemento a lo anterior, se pretende evidenciar los beneficios de un sistema de gestión de la continuidad del servicio en las diferentes perspectivas que se presentan en las organizaciones públicas y sin fines de lucro; de la misma manera que la Norma Internacional INTE/ISO 22301, se busca gestionar la capacidad de estas, para seguir funcionando durante las disrupciones. Así que desde la perspectiva:

- **De creación de valor público**: apoya los objetivos estratégicos que tiene la organización, además protege y mejora su reputación y credibilidad.
- **Normativa**: garantiza la prestación oportuna y la calidad de los servicios públicos, particularmente cuando se trata de servicios críticos, por su incidencia en el desarrollo social, económico y ambiental del país y en el funcionamiento efectivo del Estado.
- **Financiera**: aprovecha al máximo los recursos con los que se cuenta en la organización y reduce los costos directos e indirectos de las disrupciones.
- **De las partes interesadas:** enfoca a los ciudadanos; por esta razón es que dentro de sus objetivos se deben priorizar las necesidades de estos. Ahora bien, con respecto a las demás partes interesadas en el proceso, se garantiza un compromiso que permite mejorar y cumplir las metas y objetivos de la organización.
- **De los procesos internos:** mejora la capacidad para continuar brindando los servicios durante y después de los eventos disruptivos, permite controlar los riesgos de una manera eficaz y eficiente, apoya la toma de decisiones.

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

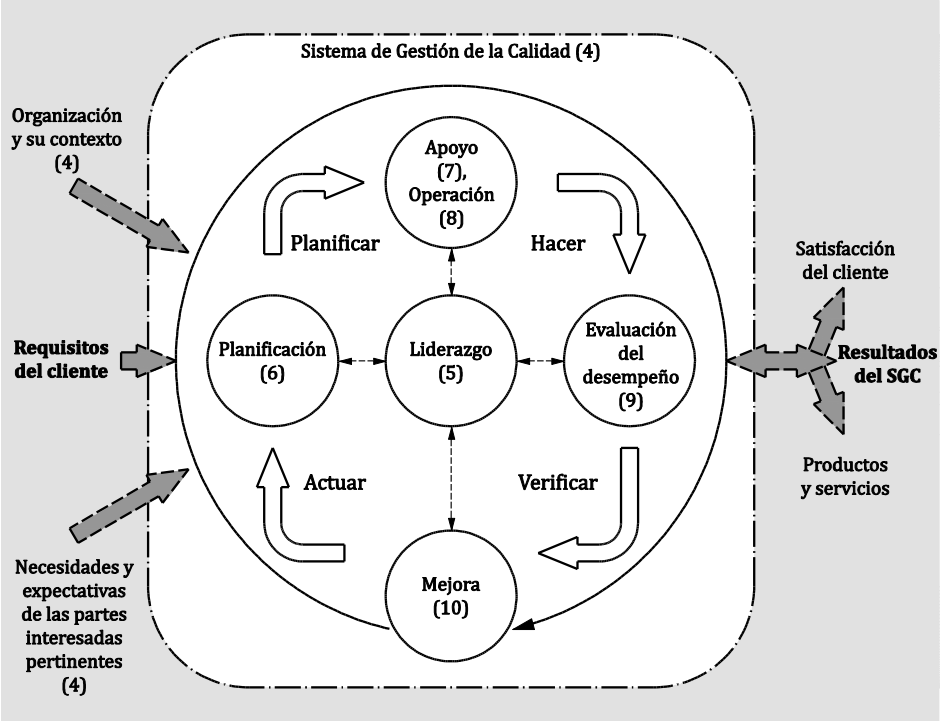
Este documento aplica el ciclo Planificar (establecer), Hacer (implementar y operar), Verificar (controlar y revisar) y Actuar (mantener y mejorar) (PHVA) para efectuar, proteger y optimar continuamente la efectividad del SGCS de una organización.

Esto garantiza un grado de coherencia con otras normas de sistemas de gestión, como la INTE/ISO 9001, la INTE/ISO 14001, la INTE/ISO 22301, la INTE/ISO/IEC 20000-1, la INTE/ISO/IEC 27001, la INTE/ISO 28000, entre otras, apoyando así la aplicación y el funcionamiento coherentes e integrados con los sistemas de gestión conexos.

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

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

- En el capítulo 5 se resumen los requisitos específicos de la función de la alta dirección en el SGCS, y la forma en que la dirección articula sus expectativas a la organización mediante una declaración de política.
- El capítulo 6 describe los requisitos para establecer los objetivos estratégicos y los principios rectores de la SGCS en su conjunto.
- El capítulo 7 apoya las operaciones de la SGCS relacionadas con el establecimiento de la competencia y la comunicación de forma recurrente o según sea necesario con las partes interesadas, a la vez que se documenta, controla, mantiene y conserva la información documentada necesaria.
- El capítulo 8 define las necesidades de continuidad de las actividades, determina cómo abordarlas y desarrolla procedimientos para gestionar la organización pública o sin fines de lucro durante una disrupción.
- En el capítulo 9 se resumen los requisitos necesarios para medir el desempeño de la continuidad del servicio, la conformidad del SGCS con este documento y la realización de una revisión de la gestión.
- El capítulo 10 identifica y actúa sobre la no conformidad del SGCS y la mejora continua mediante la adopción de medidas correctivas.



Nota. Los números entre paréntesis hacen referencia a los capítulos de esta Norma.

Figura 1 — Representación de la estructura de esta Norma con el ciclo PHVA

0.4 Contenido del presente documento

El presente documento se ajusta a los requisitos de la ISO en materia de normas de sistemas de gestión. Estos requisitos incluyen una estructura de alto nivel, un texto básico idéntico y términos comunes con definiciones básicas, diseñados para beneficiar a los usuarios que implementan múltiples normas de sistemas de gestión de la ISO.

El presente documento no incluye los requisitos específicos de otros sistemas de gestión, aunque sus elementos pueden alinearse o integrarse con los de otros sistemas de gestión.

Este documento contiene requisitos que pueden ser utilizados por una organización pública o sin fines de lucro para aplicar un SGCS y evaluar su conformidad. Una organización que desee demostrar la conformidad con este documento puede hacerlo mediante:

- una autodeterminación y una autodeclaración; o
- la confirmación de su conformidad por las partes que tienen un interés en la organización, como los clientes; o
- la confirmación de su autodeclaración por una parte externa a la organización; o
- la certificación/registro de su SGCS por una organización externa. Los capítulos 1 a 3 del presente documento establecen el alcance, las referencias normativas y los términos y definiciones que se aplican a la utilización del presente documento. En los capítulos 4 a 10 figuran los requisitos que se utilizarán para evaluar la conformidad con el presente documento. En este documento se utilizan las siguientes formas verbales:
  a) "debe" indica un requisito;
  b) "debería" indica una recomendación;
  c) "podría" indica un permiso;
  d) "puede" indica una posibilidad o una capacidad.

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

0.5 Iniciativa de esta norma

La norma INTE/ISO 22301 se enfoca específicamente en la continuidad del negocio, sin embargo, se parte de la necesidad de crear una norma nacional que su enfoque sea en la continuidad del servicio en organizaciones públicas y sin fines de lucro.

La iniciativa de esta norma INTE G130 se plantea desde el proyecto de investigación de la Universidad de Costa Rica VI-CO206 “Desarrollo de un modelo para la gestión consistente de la continuidad de los servicios en organizaciones públicas y sin fines de lucro en Costa Rica”, desarrollado desde el Centro de Investigación y Capacitación en Administración Pública en asocio con la Escuela de Administración Pública, la Escuela de Ingeniería Industrial, el Instituto Nacional de Normas de Costa Rica y la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias; quienes en conjunto elaboran la propuesta base de la norma, que posteriormente es sometida a la revisión del Comité Técnico Nacional CTN 53 SC 01, Continuidad y resiliencia.

Se pretende que esta norma sea una herramienta de utilidad pública, de uso para estas organizaciones y mejorar su cultura servicio considerando la identificación, análisis y tratamiento de riesgos bajo los principios de continuidad de las operaciones .

Sistemas de Gestión de Continuidad de Servicios para organizaciones públicas y sin fines de lucro- Requisitos y orientación para su uso.

1 OBJETO Y CAMPO DE APLICACIÓN

Este documento proporciona requisitos para que las organizaciones públicas y sin fines de lucro comprendan e implementen un sistema de gestión de la continuidad del servicio que cumpla con los requisitos homologados de la Norma Internacional INTE/ISO 22301, de forma que las organizaciones puedan desarrollar un enfoque de continuidad orientado en el servicio, con el fin de que sea una herramienta útil para la toma de decisiones en cuanto a la eficiencia en el uso de recursos y mejora en el servicio.

Promueve la implementación de un sistema de gestión de la continuidad del servicio de manera responsable y con rendición de cuentas, a través de la homologación de la Norma INTE/ISO 22301 de forma integral. Estas pautas no agregan, cambian ni modifican los requisitos de esa Norma, solamente son adaptadas al contexto de las organizaciones públicas y sin fines de lucro del país con elementos y conceptos adicionales para su mayor comprensión.

Es aplicable a todos los procesos de las organizaciones públicas y sin fines de lucro de todos los niveles (es decir, estratégico, táctico-directivo y operativo) para constituir un SGCS integral que se centre en que las organizaciones logren sus objetivos. El carácter integral de este sistema es esencial para garantizar que todas las áreas de la organización tengan un nivel específico de confiabilidad (es decir, la eficacia en la continuidad de los servicios).

Los requisitos especificados en este documento son genéricos y están destinados a ser aplicables a todas las organizaciones públicas o sin fines de lucro, o partes de éstas, independientemente del tipo, tamaño y naturaleza de la organización. El grado de aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.

Este documento es aplicable a todos los tipos y tamaños de organizaciones públicas o sin fines de lucro que:

a) implementen, mantengan y mejoren un SGCS;
b) busquen garantizar la conformidad con la política de continuidad del servicio establecida;
c) necesiten ser capaces de continuar entregando productos y servicios a una capacidad predefinida aceptable durante un evento disruptivo;
d) busquen mejorar su resiliencia a través de la aplicación efectiva del SGCS.

Este documento se puede utilizar para evaluar la capacidad de una organización para satisfacer sus propias necesidades y las obligaciones de continuidad del servicio.

Nota. Cuando la presente norma se haga referencia al término “servicio”, se hace referencia a los términos servicio público y/o sin fines de lucro.

2 NORMAS DE REFERENCIA

Las siguientes normas contienen disposiciones que, al ser citadas en este texto, constituyen requisitos de esta norma. Las ediciones indicadas estaban en vigencia en el momento de esta publicación. Como toda norma está sujeta a revisión, se recomienda a aquellos que realicen acuerdos con base a ellas, que analicen la conveniencia de usar las ediciones recientes de las normas citadas seguidamente.

INTE/ISO 22301,	Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio - Requisitos.
INTE/ISO/TS 22317,	Seguridad de la sociedad. Sistema de gestión de continuidad del negocio. Directrices para el análisis de impacto al negocio (BIA).
INTE/ISO 22300,	Seguridad y resiliencia - Vocabulario
INTE/ISO 22313,	Seguridad de la Sociedad. Sistema de Gestión de la Continuidad del Negocio (SGCN). Orientaciones.
INTE/ISO/TS 22318,	Seguridad de la sociedad. Sistema de gestión de continuidad del negocio. Directrices para continuidad de la cadena de suministros.
INTE/ISO 31000,	Gestión del riesgo - Directrices
INTE/ISO/IEC 27031,	Tecnología de la información. Técnicas de seguridad - Directrices para la tecnología y comunicación de preparación para la continuidad del negocio.
Ley No. 8488	Ley Nacional de Emergencias y Prevención del Riesgo
Ley N° 6227	Ley General de la Administración Pública
CNE-NA-INTE-DN 1	Norma de planes y preparativos de respuesta ante emergencias para centros laborales o de ocupación pública. Requisitos.

3 TÉRMINOS Y DEFINICIONES

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

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

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

Nota. Los términos y definiciones que figuran a continuación sustituyen a los que figuran en la norma INTE/ISO 22300.

3.1 actividad:

conjunto de una o más tareas con una salida definida

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

3.2 acción correctiva:

acción para eliminar la (s) causa (s) de una *no conformidad* (ver apartado 3.21) y para prevenir su recurrencia

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

3.3 actividad priorizada:

actividad (ver apartado 3.1) a la que se le asigna un nivel de urgencia para evitar *impactos* (ver apartado 3.17) inaceptables en el servicio durante un *evento disruptivo* (ver apartado 3.13)

[FUENTE: ISO 22300: 2018, 3.176, modificado - La definición ha sido reemplazada y la Nota 1 a la entrada ha sido eliminada.

3.4 alta dirección:

persona o grupo de personas que dirige y controla una *organización* (ver apartado 3.23) al más alto nivel.

Nota 1 a la entrada: La alta dirección tiene el poder de delegar autoridad y proporcionar *recursos* (ver apartado 3.30) dentro de la organización.

Nota 2 a la entrada: Si el alcance del *sistema de gestión* (ver apartado 3.36) cubre solo una parte de una organización, la alta dirección se refiere a aquellos que dirigen y controlan esa parte de la organización.

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

3.5 análisis de impacto en el servicio:

proceso (ver apartado 3.28) de análisis del *impacto* (ver apartado 3.17) en el tiempo de un *evento disruptivo* (ver apartado 3.13) en la *organización* (ver apartado 3.23).

Nota 1 a la entrada: El resultado es una declaración y justificación de los *requisitos* (ver apartado 3.31) de *continuidad del* servicio (ver apartado 3.8).

[FUENTE: ISO 22301: 2020, 3.5, modificado - La definición ha sido adaptada]

3.6 auditoría:

proceso (ver apartado 3.28) sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar en qué medida se cumplen los criterios de auditoría.

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

Nota 2 a la entrada: La *organización* (ver apartado 3.28) o una parte externa en su nombre realizan una auditoría interna.

Nota 3 a la entrada: "Evidencia de auditoría" y "criterios de auditoría" se definen en la norma ISO 19011.

Nota 4 a la entrada: Los elementos fundamentales de una auditoría incluyen la determinación de la conformidad (ver apartado 3.9) de un objeto de acuerdo con un procedimiento llevado a cabo por el personal que no es responsable del objeto auditado.

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

3.7 cliente/ciudadano:

persona u organización que podría o que recibe un *producto* o un *servicio* (ver apartado 3.29) destinado o requerido por ellos.

Nota 1 a la entrada: se incorpora el concepto de ciudadano como el vínculo de una persona con el Estado y que le permite contar con deberes y derechos.

3.8 continuidad del servicio:

capacidad de una *organización* (ver apartado 3.23) para continuar la entrega de *productos* y *servicios* (ver apartado 3.27) dentro de plazos aceptables a una capacidad predefinida durante un *evento disruptivo* (ver apartado 3.13)

[FUENTE: ISO 22301:2020, 3.3, modificado - La definición ha sido adaptada]

3.9 conformidad:

cumplimiento de un *requisito* (ver apartado 3.31)

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

3.10 competencia:

capacidad de aplicar conocimientos y habilidades para lograr los resultados previstos.

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

3.11 desempeño:

resultado medible.

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

Nota 2 a la entrada: El desempeño puede relacionarse con *actividades* (ver apartado 3.1) de gestión, *procesos* (ver apartado 3.28), productos (incluidos servicios), sistemas u *organizaciones* (ver apartado 3.23).

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

3.12 eficacia:

medida en que se realizan las *actividades* (ver apartado 3.1) planificadas y se alcanzan los resultados planificados.

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

3.13 evento disruptivo:

incidente (ver apartado 3.15), ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de *productos* y *servicios* (ver apartado 3.29) de acuerdo con los *objetivos* (ver apartado 3.22) de una *organización* (ver apartado 3.23)

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

3.14 gestión de la continuidad del servicio:

conjunto de estrategias, planes, lineamientos directrices y prácticas que permiten la continuidad institucional y del servicio público en específico, por lo que resulta fundamental sea vista como un proceso holístico, pues permite, a partir de la identificación de posibles amenazas que puedan afectar y generar una interrupción, crear un marco de resistencia.

Nota 1 a la entrada: Este concepto es tomado y utilizado por la Contraloría General de la República.

Nota 2 a la entrada: En la presente Norma se entiende interrupción como disrupción.

3.15 incidente

evento que puede ser o podría provocar un *evento disruptivo* (ver apartado 3.13), pérdida, emergencia o crisis.

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

3.16 información documentada:

información requerida para ser controlada y resguardada por una *organización* (ver apartado 3.23) y el medio en el que está contenida.

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

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

- *sistema de gestión* (ver apartado 3.36), incluidos los *procesos* (ver apartado 3.28) relacionados;
- información creada para que la organización opere (documentación);
- evidencia de resultados alcanzados (registros).

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

3.17 impacto:

resultado de un *evento disruptivo* (ver apartado 3.13) que afecta los *objetivos* (ver apartado 3.22).

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

3.18 jerarca:

superior jerárquico del órgano o del ente; ejerce la máxima autoridad dentro del órgano o ente, unipersonal o colegiado.

Nota 1 a la entrada: Este concepto es utilizado en la normativa nacional en la Ley General de Control Interno Nº8292 artículo 2.

3.19 medición:

proceso (ver apartado 3.28) para determinar un valor.

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

3.20 mejora continua:

actividad (ver apartado 3.1) recurrente para mejorar el *desempeño* (ver apartado 3.11)

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

3.21 no conformidad:

incumplimiento de un *requisito* (Ver apartado 3.31).

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

3.22 objetivo:

resultado a alcanzar.

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

Nota 2 a la entrada: Los objetivos pueden relacionarse con diferentes disciplinas (tales como metas financieras, de salud y seguridad y ambientales) y pueden aplicarse a diferentes niveles (como a nivel estratégico, de toda la organización, proyecto, producto y *proceso* (Ver apartado 3.28)).

Nota 3 a la entrada: Un objetivo puede expresarse de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, como un objetivo de *continuidad del servicio* (Ver apartado 3.8), o mediante el uso de otras palabras con un significado similar (por ejemplo, meta o propósito).

Nota 4 a la entrada: En el contexto de los sistemas de gestión de la *continuidad del servicio* (ver apartado 3.8), la *organización* (Ver apartado 3.23) establece sus objetivos de acuerdo con la política de *continuidad del servicio* (Ver apartado 3.8), para lograr resultados específicos.

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

3.23 organización

persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus *objetivos* (Ver apartado 3.22)

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

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

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

3.24 parte interesada:

persona u *organización* (ver apartado 3.23) que puede afectar, verse afectada o percibirse como afectada por una decisión o *actividad* (ver apartado 3.1)

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

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

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

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

3.25 plan de continuidad del servicio:

información documentada (ver apartado 3.16) que guía a una *organización* (ver apartado 3.23) para responder a un *evento disruptivo* (ver apartado 3.13) y reanudar, recuperar y restaurar la entrega de *productos* y *servicios* (ver apartado 3.29) de acuerdo con sus *objetivos* (ver apartado 3.22) de *continuidad del servicio* (ver apartado 3.8).

[FUENTE: ISO 22301: 2020, 3.4, modificado - La definición ha sido adaptada]

3.26 política:

intenciones y dirección de una *organización* (Ver apartado 3.23), expresada formalmente por su *alta dirección* (Ver apartado 3.4)

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

3.27 política pública:

curso o línea de acción definido para orientar o alcanzar un fin, que se expresa en directrices, lineamientos, objetivos estratégicos y acciones sobre un tema y la atención o transformación de un problema de interés público. Explicitan la voluntad política traducida en decisiones y apoyo en recursos humanos, técnicos, tecnológicos y financieros y se sustenta en los mandatos, acuerdos o compromisos nacionales e internacionales.

Nota 1 a la entrada: Este concepto es utilizado a nivel nacional por medio del Ministerio de Planificación y Política Económica (MIDEPLAN).

3.28 proceso:

conjunto de *actividades* (Ver apartado 3.1) interrelacionadas, o que interactúan, que transforman las entradas en salidas.

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

3.29 producto y servicio:

producto o resultado proporcionado por una *organización* (Ver apartado 3.23) a las *partes interesadas* (Ver apartado 3.24).

EJEMPLO Artículos manufacturados, seguros de automóviles, enfermería comunitaria.

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

3.30 recurso:

todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones y suministros e información (ya sea electrónica o no) que una *organización* (Ver apartado 3.23) tiene a disposición para usar, cuando sea necesario, para operar y cumplir con su *objetivo* (Ver apartado 3.22).

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

3.31 requisito:

necesidad o expectativa establecida, generalmente implícita u obligatoria.

Nota 1 a la entrada: “Generalmente implícito” significa que es costumbre o práctica común para la *organización* (Ver apartado 3.23) y las *partes interesadas* (Ver apartado 3.24) que la necesidad o expectativa bajo consideración esté implícita.

Nota 2 a la entrada: Un requisito especificado es uno que se establece, por ejemplo, en *información documentada* (Ver apartado 3.16).

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

3.32 riesgo:

efecto de la incertidumbre sobre los *objetivos* (Ver apartado 3.32).

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

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

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

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

3.33 seguimiento:

determinar el estado de un sistema, un *proceso* (Ver apartado 3.28) o una *actividad* (Ver apartado 3.1).

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

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

3.34 servicios críticos/servicio priorizado:

servicios públicos cuya interrupción resultaría en afectaciones altas o muy altas en el bienestar de la población y en el funcionamiento de las actividades socioeconómicas e institucionales del país.

Nota 1 a la entrada: Este concepto es tomado y utilizado por la Contraloría General de la República.

Nota 2 a la entrada: El término servicio priorizado es proveniente de la norma INTE/ISO 22301.

3.35 servicio público:

es un servicio que por su importancia para el desarrollo sostenible del país es calificado como tal por la Asamblea Legislativa, con el fin de sujetarlo a las regulaciones de la ley. Son los bienes o servicios que no pueden ser disfrutados por un individuo sin que otros tengan acceso a ellos. El disfrute del servicio público es general, y para toda la población.

Nota 1 a la entrada: Este concepto es utilizado en la normativa nacional en la Ley de la Autoridad Reguladora de Servicios Públicos Nº7593 artículo 3.

3.36 sistema de gestión:

conjunto de elementos de una **organización** (Ver apartado 3.23) interrelacionados o que interactúan para establecer políticas (Ver apartado 3.26) y *objetivos* (Ver apartado 3.22) y *procesos* (Ver apartado 3.28) para alcanzar esos objetivos.

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

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

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

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

3.37 subcontratar:

hacer un arreglo donde una *organización* (Ver apartado 3.23) externa realiza parte de la función o *proceso* (Ver apartado 3.28) de una organización.

Nota 1 a la entrada: Una organización externa está fuera del alcance del *sistema de gestión* (Ver apartado 3.36), aunque la función o proceso tercerizado esté dentro del alcance.

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

3.38 valor público:

la capacidad del Estado para dar respuesta a problemas pertinentes de la población en el marco del desarrollo sostenible, ofreciendo bienes y servicios eficientes, de calidad e inclusivos, promoviendo oportunidades, dentro de un contexto democrático.

Nota 1 a la entrada: Este concepto es tomado del Ministerio de Planificación y Política Económica en el documento Marco conceptual y estratégico para el fortalecimiento de la Gestión para Resultados en el Desarrollo en Costa Rica. 2016 p.18.

3.39 valoración del riesgo:

identificación y análisis de los riesgos que enfrenta la institución, tanto de fuentes internas como externas pertinentes para la consecución de los objetivos; deben ser realizados por el jerarca y los titulares subordinados, con el fin de determinar cómo se deben administrar dichos riesgos.

Nota 1 a la entrada: Este concepto que es utilizado en la normativa nacional en la Ley General de Control Interno Nº8292 artículo 2.

3.40 INTE/ISO:

ISO por sus siglas en inglés corresponde a la *Internacional Organization for Standardization*, (Organización Internacional de Normalización). Dicha organización es la encargada de la elaboración de normas técnicas internacionales.

INTE es el prefijo utilizado en las normas nacionales o que han sido homologadas por Instituto de Normas Técnicas de Costa Rica (INTECO) en correspondencia con normas internacionales.

4 CONTEXTO DE LA ORGANIZACIÓN

4.1 Comprensión de la organización y su contexto

La organización pública o sin fines de lucro debe determinar los asuntos externos e internos que sean pertinentes para su propósito y que afecten su capacidad para lograr los resultados previstos de su SGCS.

Nota. Estos asuntos estarán influenciados por los objetivos generales de la organización, sus productos y servicios y la cantidad y tipo de riesgo que puede o no asumir.

Las organizaciones en general se ven expuestas a un contexto interno y externo con una serie de elementos y acontecimientos que pueden afectar el cumplimiento de los objetivos. En ese sentido las organizaciones públicas y sin fines de lucro deben identificar el contexto externo en el que estas se desenvuelven.

Entre ellos: factores económicos (política fiscal y monetaria, inflación, tipo de cambio, tasas de interés, entre otros), factores políticos (asociados a temas legales, cambios y modificaciones en leyes, reglamentos, directrices) factores tecnológicos (Infraestructura de tecnología y comunicaciones, legislación sobre tecnología, y desarrollo de la competencia, investigación e innovación, regulación de la propiedad industrial e intelectual, incentivos tecnológicos entre otros).

Adicionalmente, las organizaciones se ven expuestas a diversos factores internos que pueden afectar sus operaciones si no se identifican y se generan estrategias para gestionarlos. A este nivel la organización debería identificar los elementos que pueden afectar la capacidad para lograr los resultados de la organización entre ellos: desempeño, nivel de madurez del sistema de gestión, satisfacción del ciudadano y de partes interesadas, disponibilidad de recursos, reglas y procedimientos para la toma de decisiones, competencia de las personas, organización, cultura organizacional, relaciones con sindicatos, convenciones colectivas y colaboradores en general, cumplimiento de los mandatos legales que dieron origen a su creación, entre otros.

La determinación del contexto significa una herramienta importante para las organizaciones ya que facilita la toma de decisiones. Para ello es necesario la incorporación y participación de diversas unidades dentro de la organización con el fin de conocer diferentes puntos de vista y se obtenga un resultado más amplio. Lo anterior permite la generación de estrategias de resolución de problemas y mejora continua.

4.2 Comprender las necesidades y expectativas de las partes interesadas

4.2.1 Generalidades.

Al establecer su SGCS, la organización pública o sin fines de lucro debe determinar:

a) las partes interesadas que son pertinentes para el SGCS;

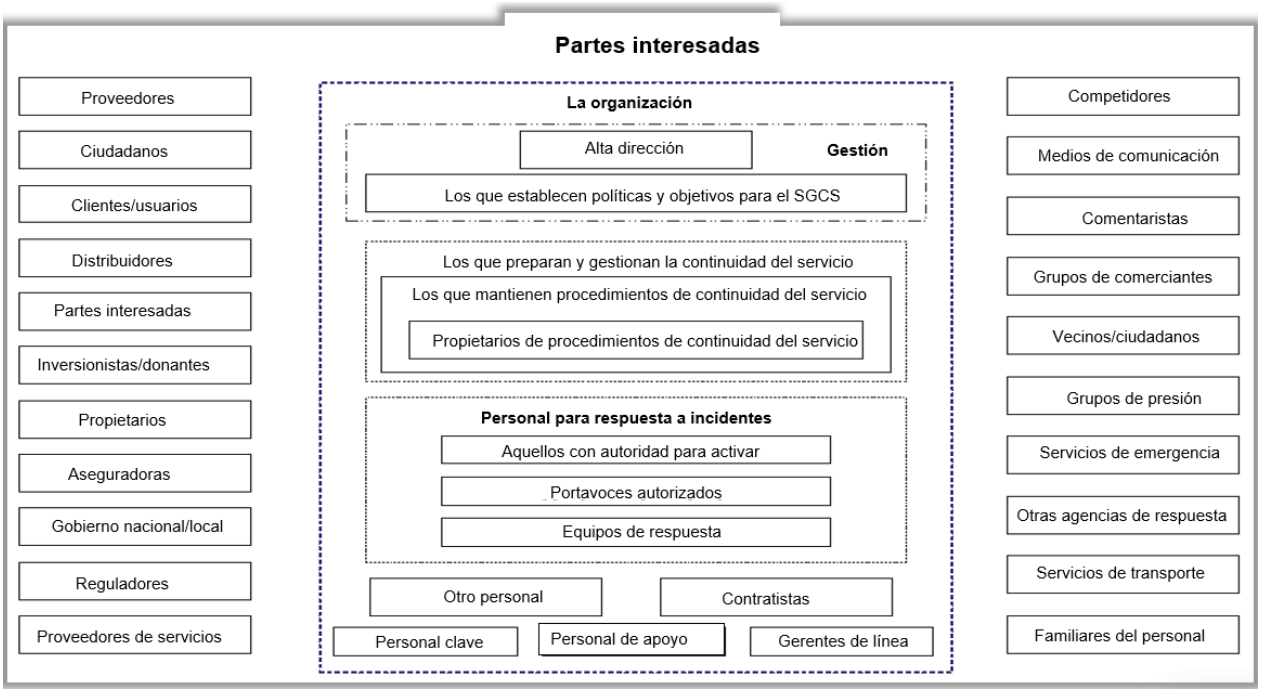
b) los requisitos pertinentes de estas partes interesadas.

Las organizaciones públicas y sin fines de lucro deberían identificar a individuos, grupos u organizaciones en el sector público, privado o sociedad civil organizada a nivel nacional, regional o internacional que sean pertinentes para el sistema de gestión de la continuidad del servicio, con el fin de conocer sus necesidades y expectativas. Algunos ejemplos de partes interesadas que se pueden mencionar son: organizaciones públicas, asociaciones de desarrollo, grupos o comités regionales, municipales o locales, academia, organizaciones no gubernamentales, proveedores externos, usuarios de los servicios entre otros a nivel nacional e internacional.

Para la identificación de las partes interesadas en el sistema (ver ejemplos de partes interesadas en la figura 2), es necesario realizarlo de manera conjunta por todas las áreas de la organización, esto con el fin de conocerlas desde diferentes perspectivas y que el proceso sea de forma participativa dada las particularidades de cada área de esta. Para ello se recomienda la realización de talleres participativos donde todos los niveles de la organización sean involucrados en el proceso con el objetivo de identificarlas adecuadamente, así como los requisitos y expectativas de estas.

En ese sentido, los pasos para la identificación de las partes interesadas pertinentes son los siguientes:

a. Realizar una lista con la identificación de las partes interesadas, esto por medio de sesiones con la participación de las áreas de la organización.
b. Valorar si la lista obtenida corresponde a partes interesadas. Algunas preguntas orientadoras para su determinación pueden ser las siguientes:
   ¿Existen posibilidades de que la parte interesada pueda pausar las operaciones de la organización?
   ¿Es posible que la parte interesada modifique nuestro proceso o nuestros bienes o servicios?
   ¿Es posible que la parte interesada colabore en el largo plazo con la visión de la organización?
c. Definir los requisitos pertinentes o expectativas de las partes interesadas. Para ello también será necesario realizar talleres, entrevistas o encuestas para verificar con cada una de las partes sus intereses y que la organización la determine finalmente como una parte interesada pertinente.



Fuente: Adaptada de la norma INTE/ISO 22313

Figura 2. Ejemplos de partes interesadas a considerar en sectores públicos y organizaciones sin fines de lucro (cambiar inversionistas/donantes)

4.2.2 Requisitos legales y reglamentarios
La organización pública o sin fines de lucro debe:
a) implementar y mantener un proceso para identificar, tener acceso y evaluar los requisitos legales y reglamentarios aplicables relacionados con la continuidad de sus servicios, actividades y recursos;
b) garantizar que estos requisitos legales, reglamentarios y de otro tipo se tengan en cuenta al implementar y mantener su SGCS;
c) documentar esta información y mantenerla actualizada.

Las organizaciones públicas y sin fines de lucro deberían determinar los requisitos legales y reglamentarios asociados a las partes interesadas identificadas previamente. El alcance de estos debe ir alineado a su mandato, los productos y servicios públicos que normalmente se proporcionan de acuerdo con el marco normativo aplicable. Las organizaciones deberían determinar la aplicabilidad de los requisitos de este documento de acuerdo con el alcance de su sistema de gestión y deberían mantenerse como información documentada de manera transparente y actualizada.

Las organizaciones públicas y sin fines de lucro por su naturaleza están sujetas a una serie de normativas que van a determinar su marco de actuación. En ese sentido la definición de requisitos legales es clave para el éxito del modelo. Uno de los aspectos a considerar por parte de las organizaciones, es que la continuidad de los servicios se encuentra estipulado en el marco normativo del país, específicamente en la Ley General de la Administración Pública, que establece que los servicios públicos deben regirse por el principio de continuidad del servicio: la actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su continuidad, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios (Ley N° 6227 art.4).

4.3 Determinar el alcance del SGCS

4.3.1 Generalidades

La organización pública y sin fines de lucro debe determinar los límites y la aplicabilidad del SGCS para establecer su alcance; para determinar este, la organización debe considerar:

a) las cuestiones externas e internas mencionadas en el apartado 4.1;
b) los requisitos mencionados en el apartado 4.2;
c) su misión, visión, objetivos y obligaciones internas y externas.

El alcance debe estar disponible como información documentada.

4.3.2 Alcance del SGCS

La organización pública o sin fines de lucro debe:

a) establecer las partes de la organización que se incluirán en el SGCS, teniendo en cuenta su ubicación, tamaño, naturaleza y complejidad;
b) identificar los servicios que se incluirán en el SGCS.

Al definir el alcance, la organización debe documentar y explicar las exclusiones. Estas no deben afectar la capacidad y la responsabilidad de la organización de proporcionar continuidad del servicio, según lo determinado por el análisis de impacto en el servicio o la evaluación de riesgos y los requisitos legales o reglamentarios aplicables.

Las organizaciones deberían utilizar el plan estratégico, plan de desarrollo, o el máximo instrumento de planificación como base para delimitar el sistema de gestión, tomando en cuenta el marco estratégico de la organización entendido este como los objetivos estratégicos, misión, visión, entre otros elementos considerados en la planificación.

Aunado a ello, las organizaciones deberían considerar el marco normativo donde se definen las competencias y su marco de acción para el cumplimiento de los objetivos. Es necesario valorar elementos tales como su naturaleza jurídica, tamaño de la organización, recurso humano disponible, aspectos presupuestarios y elementos propios de la planificación institucional.

La organización debería identificar los responsables a lo interno de dirigir el sistema de gestión de continuidad, el cual le dará seguimiento a este.

En apego a su marco de competencias debería definir los servicios que se incluirán en el sistema de gestión de la continuidad del servicio, estos deben ser priorizados de acuerdo con el ámbito de acción de la organización, de la obligatoriedad según el marco normativo o del tipo de servicio público que entrega al ciudadano. En ese sentido la identificación de los servicios deberá realizarse de forma participativa con el involucramiento de todos los niveles de la organización (nivel político, directivo, departamental y operacional).

4.4 Sistema de Gestión de Continuidad de Servicios (SGCS)

La organización pública y sin fines de lucro debe establecer, implementar, mantener y mejorar continuamente un SGCS, incluidos los procesos necesarios y sus interacciones, de acuerdo con los requisitos de este documento.

La organización debería garantizar la continuidad del SGCS al cambiar la administración, garantizando una entrega oportuna y completa de toda la información sobre los proyectos y planes en curso, así como el contenido y el estado del sistema.

La organización debería mantener información documentada sobre los procesos de su SGCS, con el propósito de lograr un desempeño eficaz y transparente. Esta información debería estar disponible y accesible a través de textos, formatos electrónicos, fotografías o cualquier otro medio para probar que los procesos se llevan a cabo según lo planificado.

La alta dirección debería asignar a las personas la responsabilidad y la autoridad para liderar el desarrollo y mantenimiento continuo del SGCS. Los procesos deberían revisarse regularmente para evaluar su efectividad y para planificar un mejor desempeño del sistema de gestión de la continuidad del servicio.

Los procesos dentro de la organización pública o sin fines de lucro deberían definirse como entradas, actividades y salidas, incluidas las interfaces con otros procesos, rendición de cuentas y responsabilidades para estos, los cuales deben estar alineados al Plan Estratégico o de Desarrollo de la organización.

5 LIDERAZGO

5.1 Liderazgo y compromiso

La alta dirección debe demostrar liderazgo y compromiso con respecto al SGCS al:

a) asegurar que la política y los objetivos de continuidad del servicio estén establecidos y sean compatibles con la dirección estratégica de la organización;
b) asegurar la integración de los requisitos del SGCS en los procesos de servicio de la organización;
c) asegurar que los recursos necesarios para el SGCS estén disponibles;
d) comunicar la importancia de la continuidad efectiva del servicio y de cumplir con los requisitos del SGCS;
e) asegurar que el SGCS logre los resultados previstos;
f) dirigir y apoyar a las personas para que contribuyan a la efectividad del SGCS;
g) promover la mejora continua;
h) apoyar otros roles gerenciales pertinentes para demostrar su liderazgo y compromiso en lo que respecta a sus áreas de responsabilidad.

Nota. La referencia a "servicio" en este documento puede interpretarse de manera amplia para referirse a aquellas actividades que son fundamentales para los propósitos de la existencia de la organización pública y sin fines de lucro.

Una vez establecido el contexto y fijado el alcance del Sistema de Gestión de la Continuidad del Servicio (SGCS), es importante hacer énfasis en el equipo necesario que ayudará a que la implementación de este tenga éxito.

El capítulo 5 da énfasis en el mandato de la alta jerarquía de la organización para que establezca un marco de compromisos y genere liderazgo con el SGCS. Lo anterior es esencial en la implementación de un sistema de gestión, ya que respalda ante toda la organización las decisiones y las estrategias que se deriven.

Las organizaciones en general cuentan con objetivos determinados en la prestación de servicios y deben ir orientados a la generación de valor público. En ese sentido, el destinar recursos a la gestión del riesgo en las organizaciones en ocasiones no es una prioridad, por lo cual es necesario que la alta jerarquía comunique de forma efectiva a toda la organización los beneficios de mediano y largo plazo de la implementación de un marco de la continuidad del servicio ante la concreción de un evento disruptivo.

Por tanto, es necesario asegurar que la política y los objetivos de continuidad del servicio estén establecidos y sean compatibles con la dirección estratégica de la organización, para ello las

organizaciones públicas y sin fines de lucro deberían establecer una declaración pública y transmitir a la organización y los terceros interesados que este liderazgo y compromiso se puede demostrar.

Para la ejecución e implementación del SGCS es necesario la definición de recursos, lo que son limitados en el sector público, por lo que cobra relevancia su asignación y justificación para que la alta dirección realice el compromiso de asignación del equipo responsable que coordine el proceso con responsabilidades claras y medición del desempeño de la continuidad del servicio y su nivel de desarrollo.

5.2 Política

5.2.1 Establecer la política de continuidad del servicio

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

a) sea apropiada para el propósito de la organización pública o sin fines de lucro;
b) proporcione un marco de referencia para establecer objetivos de continuidad del servicio;
c) incluya un compromiso para satisfacer los requisitos aplicables;
d) incluya un compromiso de mejora continua del SGCS.

La política de continuidad del servicio debería ser una guía de principios y un compromiso de parte de la organización en la cual se establecen los objetivos del SGCS; esta debería establecer el compromiso de la organización para la implementación del SGCS y que promueva la mejora continua de los procesos. También debería considerar el marco normativo de la organización, y toda aquella normativa relacionada con sus actividades.

La alta dirección de la organización debe ser la responsable de elaborar la política de continuidad del servicio, de forma que se cuente con un respaldo desde la parte estratégica de la organización para el resto de las unidades organizacionales. La política debería servir como marco de referencia para desarrollar, implementar y actualizar, cuando sea necesario, los objetivos de continuidad del servicio. Por lo tanto, debería proporcionar criterios de alto nivel para los procesos de toma de decisiones. Asimismo, la política debería revisarse periódicamente para mantener su consistencia con la mejora continua del SGCS.

De esta forma, la política de continuidad del servicio en las organizaciones públicas y sin fines de lucro debería contar con al menos los siguientes requisitos:

a. El aval de la alta dirección
b. Estar por escrito y contener los siguientes elementos: objetivos, obligaciones de la organización respecto a la continuidad del servicio, alcance, limitaciones y las partes de la organización que quedan excluidas.
c. Un contexto normativo (leyes, reglamentos y otros) que se encuentran relacionados con la continuidad de los servicios.

Nota. Ver el anexo B para más información sobre el marco normativo a considerar sobre continuidad de los servicios.

a. Si la organización ya cuenta con un sistema de gestión operando, el SGCS debería incorporarse.
b. La política de continuidad debe contar con el compromiso de la mejora continua.
c. Establecer los responsables dentro de la organización de la continuidad del servicio, sus roles, asignaciones y forma de medición del desempeño, por ejemplo, un informe. Se recomienda asignar las responsabilidades según su rol, como, por ejemplo: “oficial de continuidad del servicio”, “coordinador del proceso de continuidad’’, o bien, crear una “Comisión o Comité de Continuidad del Servicio” que brinde seguimiento al proceso y mantener el SGCS en toda la organización.

5.2.2 Comunicación de la política de continuidad del servicio

La política de continuidad del servicio debe:

a) estar disponible como información documentada;
b) ser comunicada dentro de la organización;
c) estar disponible para las partes interesadas, según corresponda.

La política de continuidad del servicio debe comunicarse y estar disponible a nivel de toda la organización, así como para las partes interesadas y la ciudadanía en general, con el fin de comunicarla de la mejor forma; se recomienda utilizar algunos de los siguientes canales:

a. Página web de la organización
b. Reuniones, capacitaciones, talleres, charlas.
c. Intranet
d. Videos informativos
e. Afiches, memorándums, cartas de compromiso
f. Avisos por medio de correos electrónicos
g. Grupos de trabajo organizados en plataformas tecnológicas
h. Entre otros.

5.3. Roles, responsabilidades y autoridades

La alta dirección debe garantizar que las responsabilidades y autoridades para los roles pertinentes se asignen y comuniquen a lo interno de la organización, además debe asignar la responsabilidad y la autoridad para:

a) asegurar que el SGCS cumpla con los requisitos de este documento;
b) informar sobre el desempeño del SGCS a la alta dirección.

La alta dirección debe definir y comunicar las responsabilidades de los colaboradores de la organización y a la vez asegurar que se comprendan para su realización.

Las responsabilidades y autoridades asignadas deberían:

- Garantizar que el SGCS cumpla con los requisitos de este documento.
- Asegurar el compromiso de la alta dirección.
- Dar seguimiento a los objetivos planteados en la política de continuidad del servicio y verificar que se cumplan.
- Definir canales de comunicación y divulgación de la información, avances, resultados del SGCS en toda la organización.
- Priorizar en todos los procesos de la organización pública o sin fines de lucro un enfoque de creación de valor público para continuar brindando los servicios públicos de forma oportuna, eficaz y eficiente.

Para estas responsabilidades, la organización debería conformar una “Comisión o Comité de Continuidad del Servicio” que brinde seguimiento al proceso y mantenga el SGCS en toda la organización.

6 PLANIFICACIÓN

6.1 Acciones para abordar riesgos y oportunidades

6.1.1 Determinando riesgos y oportunidades

Al planificar el SGCS, la organización pública y sin fines de lucro debe considerar los asuntos mencionados en el apartado 4.1 y los requisitos mencionados en el apartado 4.2 y determinar los riesgos y oportunidades que deben abordarse para:

a) asegurar que el SGCS pueda lograr su(s) resultado(s) deseado(s);
b) prevenir o reducir los efectos no deseados;
c) lograr la mejora continua.

La implementación del SGCS requiere una etapa de planificación, en la cual se definan los riesgos y oportunidades que necesitan ser gestionados. En esta etapa es necesario el abordaje de un pensamiento basado en riesgo, considerando contexto y las expectativas para implementar el SGCS con un enfoque de mejora continua, garantizando que los objetivos sean cumplidos.

La etapa de planificación debe considerar al menos:

a. La información de contexto de la organización (4.1), las necesidades identificadas y las expectativas (4.2) de las personas ciudadanas.
b. La incorporación y aseguramiento de los resultados que se han propuesto se cumplan.
c. La identificación de los riesgos y oportunidades que implican la implementación de un proyecto para un SGCS.

Nota. Algunos ejemplos de riesgos y oportunidades pueden ser los siguientes: poca disponibilidad de recursos, dificultad de contar con información, insatisfacción de los usuarios por los servicios, falta de compromiso de la alta dirección. Estos van a depender de la naturaleza de la organización.

6.1.2 Abordar riesgos y oportunidades

La organización debe planificar:

a) acciones para abordar estos riesgos y oportunidades;
b) cómo:
1) integrar e implementar las acciones en los procesos del SGCS (ver apartado 8.1);
2) evaluar la eficacia de estas acciones (ver apartado 9.1).

Nota. Los riesgos y las oportunidades se relacionan con la eficacia del sistema de gestión; los relacionados con eventos disruptivos del servicio se abordan en el apartado 8.2.

6.2. Objetivos de continuidad del servicio y planificación para alcanzarlos

6.2.1 Estableciendo los objetivos de continuidad del servicio

La organización pública y sin fines de lucro debe establecer objetivos de continuidad del servicio en funciones y niveles pertinentes, estos deben:

a) ser coherentes con la política de continuidad del servicio;
b) ser medibles (si es posible);
c) tener en cuenta los requisitos aplicables (ver apartados 4.1 y 4.2);
d) ser sujetos de seguimiento;
e) ser comunicados;

f) estar actualizados según corresponda.

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

En la etapa de planificación se deben definir objetivos de continuidad del servicio, se recomienda que estos cumplan con los requisitos del acrónimo en inglés SMART, entendido como: específicos, medibles, alcanzables, pertinentes y con un horizonte temporal.

De esta forma los objetivos planteados deberían ser:

a. **Específicos:** ser claros, contar con un alcance y ser delimitados en la medida de lo posible de acuerdo con las competencias de la organización.
b. **Medibles:** expresarse de forma que puedan medirse e identificar el avance en el cumplimiento.
c. **Alcanzables:** implicar un reto para la organización, sin embargo, es necesario que sean realistas y posibles de realizar.
d. **Pertinentes:** es importante que estén planteados y alineados a la estrategia de la organización, a su misión y visión, con el fin de que sean una prioridad para su realización.
e. **Horizonte temporal:** implica la definición del plazo en el que se cumplirán los objetivos, las prioridades y los plazos del periodo de evaluación.

Dichos objetivos deben establecerse por escrito y definir su forma de medición para evaluar el desempeño durante y después del proyecto de continuidad del servicio.

6.2.2 Determinando los objetivos de continuidad del servicio

Al planificar cómo lograr sus objetivos de continuidad del servicio, la organización pública y sin fines de lucro debe determinar:

a) lo que se hará;
b) qué recursos se requerirán;
c) quién será responsable;
d) cuándo se completará;
e) cómo se evaluarán los resultados.

Los objetivos deben venir alineados a la política de continuidad de la organización; estos deberían ser revisados de forma regular ante posibles cambios del contexto con el fin de identificar ajustes en pro de la mejora continua.

Como desarrollo de la mejora continua se debe incorporar una referencia al avance en el SGCS pensando y dejando por escrito qué persiguen estas mejoras, qué recursos estarán disponibles y quiénes serán responsables.

Para la definición de los objetivos se recomienda que sean diseñados con la metodología SMART (6.2.1).

Con el fin de definir dichos objetivos y darles seguimiento se deben incluir los siguientes elementos:

- Definir qué es lo que se va a realizar.
- Cuáles son los recursos que se requieren para cumplir con el objetivo.
- Quién o quiénes serán las personas responsables de cumplir con dicho objetivo.
- Cuál es el periodo que se utilizará para su cumplimiento;
- Cuál es la forma de dar seguimiento al indicador, para ello es necesario el establecimiento de plazos para realizar el monitoreo de los resultados definidos en el indicador.

6.3 Planificando los cambios en el SGCS

Cuando la organización pública o sin fines de lucro determina la necesidad de cambios en el SGCS, incluidos los identificados en el capítulo 10, estos se deben llevar a cabo de manera planificada y la organización debe considerar:

a) el propósito de los cambios y sus potenciales consecuencias;
b) la integridad del SGCS;
c) la disponibilidad de recursos;
d) la asignación o reasignación de responsabilidades y autoridades.

En caso de contar con cambios en el SGCS, y al considerar este tema como un proyecto, es necesario realizar una planificación para ejecutar los cambios, para lo cual es necesario la caracterización de los siguientes elementos:

a. Definir el objetivo del cambio, las razones por las cuales se desea realizar y las consecuencias que este conlleva en caso de concretarse.
b. Considerar los diversos temas que se abordan en el SGCS con el fin de asegurar su integralidad.
c. Definir los recursos (financieros, tecnológicos, humanos, entre otros) que se requieren para cumplir con el objetivo.
d. Quién o quiénes serán las personas responsables, equipo de trabajo para cumplir con dicho objetivo.

7 SOPORTE

7.1 Recursos

La organización pública o sin fines de lucro debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGCS.

Para la implementación de un SGCS es necesario contar con los siguientes recursos:

a. **Humanos:** designar las personas, las responsabilidades y el tiempo necesario al tema de la continuidad del servicio en la organización. Para ello, debe contar con personal capacitado en el tema, apoyo de la alta dirección y un proceso continuo de capacitación en el tema. Se requiere contemplar el tiempo para el desarrollo del plan de continuidad y su seguimiento, así como el sistema de gestión para la documentación.
b. **Económicos:** es necesario la asignación de presupuesto anual apropiado para el desarrollo de las actividades del SGCS.
c. **Materiales:** infraestructura, materiales y equipo para la realización y organización de los espacios de trabajo y todos los recursos necesarios para que la actividad se pueda desarrollar de forma correcta.

Para el seguimiento del SGCS es necesario que se cuente con mecanismos para hacerlo de conocimiento de la organización, por lo que se recomienda:

a. Un programa de capacitación y concientización dirigido a todas las personas trabajadoras de la organización (alta dirección, colaboradores de todos los niveles), proveedores y otras partes interesadas.
b. Un programa de comunicación y divulgación de la política de continuidad del servicio con el fin de promover la cultura de gestión del riesgo enfocado en aumentar la resiliencia organizacional, minimizar la probabilidad y el impacto de las disrupciones, e inspirar confianza a la ciudadanía.
c. Realizar talleres, declaraciones, simulacros, simulaciones con el fin de comunicar y capacitar a las partes interesadas; es importante documentar las actividades que se realicen, por ejemplo, las listas de asistencia, fotografías, notas conceptuales, programas entre otros; que permitan fortalecer capacidades en la organización.

7.2 Competencia

La organización pública o sin fines de lucro debe:

a) determinar la competencia necesaria de la(s) persona(s) que realiza(n) el trabajo bajo su control y que afecta su desempeño de la continuidad del servicio;
b) asegurar que estas personas sean competentes sobre la base de una educación, capacitación o experiencia apropiadas;
c) cuando corresponda, tomar medidas para adquirir la competencia necesaria y evaluar la eficacia de las acciones tomadas;
d) conservar información documentada apropiada como evidencia de la competencia.

Nota. Las acciones aplicables pueden incluir, por ejemplo, la provisión de capacitación, la tutoría o la reasignación de personas actualmente empleadas; o el reclutamiento o contratación (a plazo definido) de personas competentes.

7.3 Toma de conciencia

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

a) la política de continuidad del servicio;
b) su contribución a la eficacia del SGCS, incluidos los beneficios de un mejor desempeño de la continuidad del servicio;
c) las implicaciones de no cumplir con los requisitos del SGCS;
d) su propio rol y responsabilidades antes, durante y después de los eventos disruptivos.

7.4 Comunicación

La organización pública y sin fines de lucro debe determinar las comunicaciones internas y externas pertinentes para el SGCS, que incluyen:

a) lo que se comunicará;
b) cuándo comunicarlo;
c) a quién comunicarlo;
d) cómo comunicarlo;
e) quién lo comunicará.

La organización debería contar con diferentes mecanismos de comunicación tanto a nivel interno como externo dirigidas a las partes interesadas.

Para realizar las comunicaciones se recomienda lo siguiente:

a. Planificar y seleccionar la información que será comunicada a las partes interesadas de la organización.
b. Definir cómo se hará (mecanismo), cuándo se realizará, quién realizará la comunicación, para lo cual es recomendable la designación de una persona encargada de la comunicación (portavoz).
c. En el momento en que se concrete un evento disruptivo, el equipo o Comité/Comisión de Continuidad del Servicio debe nombrar a una persona responsable para que transmita toda la información que la organización considere oportuno comunicar. Estos criterios deberían estar establecidos de manera previa.
d. Para establecer un sistema de comunicación hay que tener en cuenta las expectativas de las partes interesadas y qué necesitan saber en cada momento.
e. Informar sobre la implementación y del desarrollo del sistema de continuidad del servicio en los reportes financieros como parte del sistema de concientización de la alta dirección.

Todos los documentos y las comunicaciones de los sistemas de continuidad de servicios deberían controlarse por tratarse de información sensible de la organización. En ese sentido, es necesario que la organización predefina la información a publicar.

7.5 Información documentada

7.5.1 Generalidades

El SGCS de la organización pública y sin fines de lucro debe incluir:

a) información documentada requerida por esta norma;
b) información documentada determinada como necesaria por la organización para la eficacia del SGCS.

Nota. El alcance de la información documentada para un SGCS puede diferir de una organización a otra debido a:

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

La organización debería contar con información documentada como parte del sistema de gestión de continuidad, para esto es necesario dejar evidencias del cumplimiento de los requisitos. Los documentos y procedimientos deberían incluir el nombre, la identificación y su descripción, el formato y tener prevista una revisión y una aprobación en caso de ser necesario.

La información documentada del sistema de gestión de la continuidad del servicio está formada por:

- La comprensión de la organización y su contexto
- Los requerimientos legales y reglamentarios
- El alcance del sistema de continuidad del servicio y sus exclusiones
- La política de continuidad del servicio
- Los objetivos de continuidad del servicio y la estrategia y planes para alcanzarlos
- Las competencias de las personas trabajadoras
- El análisis de impacto del servicio y la evaluación de riesgos
- Las estrategias de continuidad del servicio y las soluciones
- Los planes de continuidad y sus procedimientos
- Un programa de ejercicios
- La monitorización, medición, análisis y evaluación
- La auditoría interna
- La revisión de los responsables
- Las no conformidades y las acciones correctivas

7.5.2 Crear y actualizar

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

a) la identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);
b) el formato (por ejemplo, idioma, versión de software, gráficos) y medios (por ejemplo, papel, electrónico);
c) la revisión y aprobación de idoneidad y adecuación

7.5.3 Control

7.5.3.1 La información documentada requerida por el SGCS y por esta norma se debe controlar para garantizar que:

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

b) está adecuadamente protegida (por ejemplo, contra la pérdida de confidencialidad, uso indebido o pérdida de integridad).

7.5.3.2 Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda:

a) distribución, acceso, recuperación y uso;
b) almacenamiento y preservación, incluida la preservación de la legibilidad;
c) control de cambios (por ejemplo, control de versiones);
d) retención y disposición.

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

Nota. El acceso puede implicar una decisión con respecto al permiso para ver solo la información documentada, o el permiso y la autoridad para ver y cambiar la información documentada.

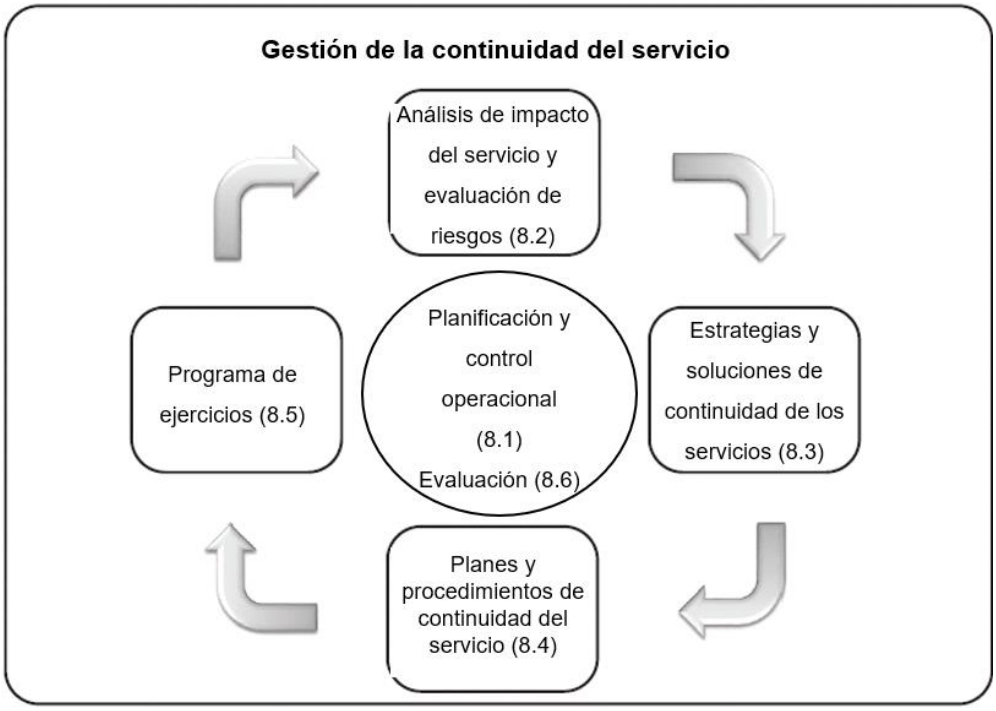
8 OPERACIÓN

8.1 Planificación y control operacional

La organización pública y sin fines de lucro debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en el apartado 6.1:
a) estableciendo criterios para los procesos;
b) implementando el control de los procesos de acuerdo con los criterios;
c) manteniendo la información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo planeado.
La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no intencionados, tomando medidas para mitigar los efectos adversos, según sea necesario.
La organización pública y sin fines de lucro debe asegurar que los procesos subcontratados y la cadena de suministro estén controlados.

El SGCS, como un nuevo proceso dentro de las organizaciones públicas y sin fines de lucro, debería ser considerado en el plan estratégico o en el plan de desarrollo de la organización (ver figura 3). Para ello debería:

a. Determinar los requisitos de los procesos priorizados que aseguren la continuidad del servicio.
b. Identificar los riesgos de cada producto y servicio.
c. Comunicar las actividades necesarias para gestionar los riesgos identificados en el punto b.
d. Determinar las personas y responsabilidades para la realización de las actividades del proceso.
e. Definir los recursos necesarios para la realización de las actividades.
f. Evaluar la forma en la que se están realizando los procesos y su efectividad en la gestión de los riesgos para la continuidad del servicio.



Fuente: Adaptada de la norma INTE/ISO 22313

Figura 3. Elementos de la gestión de la continuidad del servicio

8.2. Análisis de impacto en el servicio y evaluación de riesgos

8.2.1 Generalidades

La organización pública y sin fines de lucro debe:

a) implementar y mantener procesos sistemáticos para analizar el impacto en el servicio y evaluar los riesgos de disrupción;
b) revisar el análisis de impacto en el servicio y la evaluación de riesgos a intervalos planificados y cuando haya cambios significativos dentro de la organización o el contexto en que opera.

Nota. La organización pública y sin fines de lucro determina el orden en que se llevan a cabo el análisis de impacto en el servicio y la evaluación de riesgos.

Una vez finalizada la fase de Planificación y control operacional, es necesario que la organización ejecute las acciones para analizar el impacto en el servicio y la respectiva evaluación del riesgo de disrupción.

Para asegurar la continuidad de servicio es necesario priorizar qué productos y servicios deben seguir siendo suministrados a un determinado nivel para mitigar el impacto de un evento disruptivo. Esta priorización se puede realizar tras un proceso de análisis de impacto en el servicio donde se analicen las acciones, actividades y dependencias para poder priorizar en cuáles de ellos actuar.

Cuando se haya realizado el análisis de impacto del servicio y evaluado los riesgos de disrupción, esto brindará insumos a la organización para que definan la o las estrategias para dar respuestas a eventos disruptivos.

8.2.2 Análisis de impacto en el servicio

La organización pública y sin fines de lucro debe utilizar el proceso para analizar los impactos en el servicio para determinar las prioridades y requisitos de continuidad del servicio. El proceso debe:

a) definir los tipos de impacto y los criterios pertinentes para el contexto de la organización;
b) identificar las actividades que apoyan la provisión de productos y servicios;
c) utilizar los tipos y criterios de impacto para evaluarlos a lo largo del tiempo como resultado de la disrupción de estas actividades;
d) identificar el marco de tiempo dentro del cual los impactos de no reanudar las actividades serían inaceptables para la organización;

Nota 1. Este plazo puede denominarse "período máximo de disrupción tolerable (MTPD, por sus siglas en inglés)".

e) establecer marcos de tiempo priorizados dentro del tiempo identificado en d) para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada;

Nota 2. Este marco de tiempo puede denominarse " tiempo objetivo de recuperación (RTO, por sus siglas en inglés)".

f) utilizar este análisis para identificar actividades priorizadas;
g) determinar cuáles recursos son necesarios para apoyar actividades priorizadas;
h) determinar las dependencias, incluidos los socios y proveedores, y las interdependencias de las actividades priorizadas.

El análisis de impacto del servicio tiene como objetivo identificar las consecuencias que tendría la concreción de un evento disruptivo en una organización. De esta forma, la utilidad de ese análisis consiste en que permite que la organización conozca el impacto ante un evento disruptivo y pueda priorizar los procesos y actividades para disminuir el impacto mediante la definición de estrategias.

Para ello, es necesario definir los requisitos previos, los cuales deberían ser los siguientes:

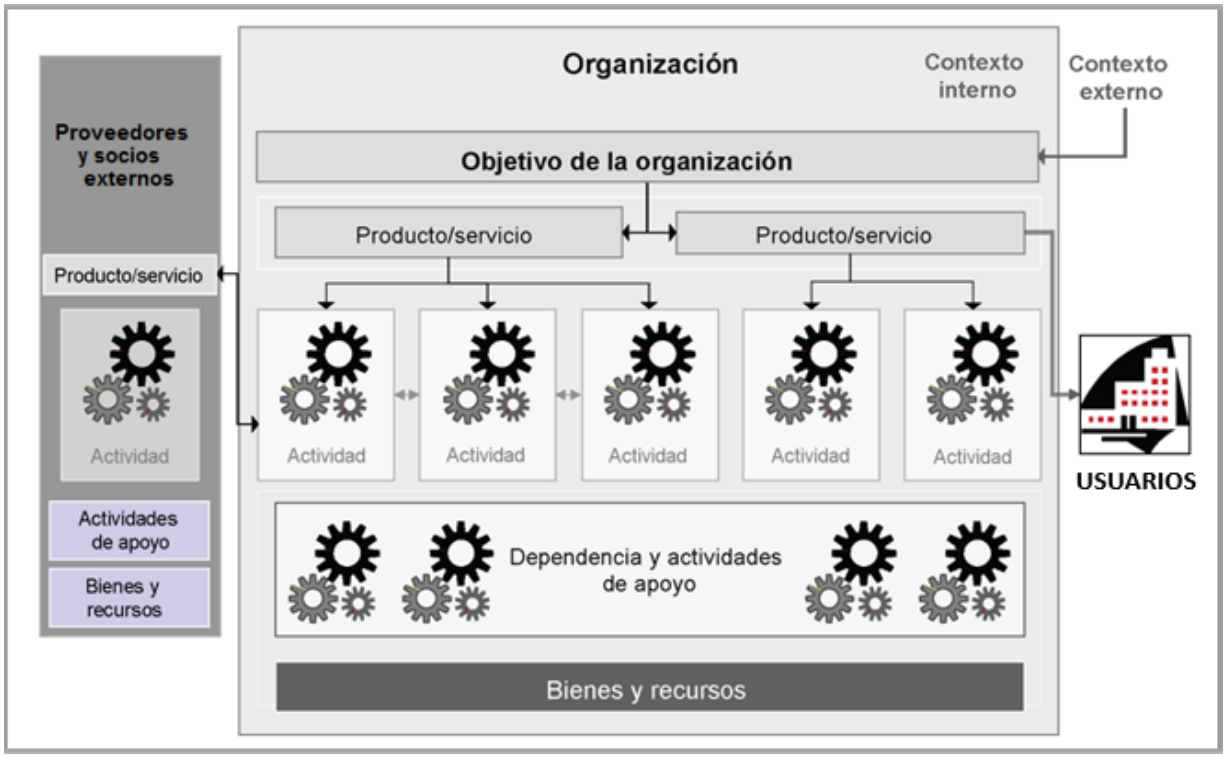
a. Definir el contexto de la organización pública o sin fines de lucro
b. Definir el alcance del proceso de continuidad del servicio.
c. Establecer los roles y las responsabilidades para asegurar la continuidad de los servicios
d. Contar con el compromiso de la alta dirección o jerarquía de la organización.
e. Definir y dotar los recursos necesarios para la realización del proceso.

Nota. En el anexo C se enlista una serie de preguntas que permiten una mejor comprensión de los requisitos previos.

El proceso para la elaboración del Análisis de Impacto del Servicio (SIA, por sus siglas en inglés) tiene como objetivo clasificar los recursos de la organización para que se pueda continuar brindando los servicios a niveles predefinidos aceptables posterior a un evento disruptivo. Para ello, se deberían seguir los siguientes pasos:

a. Al ser los servicios salidas de un proceso, se deberían establecer una serie de prioridades basadas en parámetros de tiempo.
b. Priorizar los productos o servicios: lo anterior brinda la orientación de tiempo y nivel de servicio que se desea generar.
c. Contar con el aval y consenso de la máxima jerarquía de la organización con respecto a la priorización del paso anterior.
d. Analizar los procesos y las actividades que lo componen y los recursos necesarios

El análisis debería cubrir todas las actividades dentro del alcance del SGCS. Es aceptable realizar el análisis sobre grupos de actividades, por ejemplo, relacionadas con productos y servicios específicos (ver Figura 4).



Fuente: Adaptada de la norma INTE/ISO 22313

Figura 4 - Comprensión de la organización

A continuación, se describen la serie de pasos recomendados para realizar el Análisis de Impacto del Servicio (SIA):

a. Priorización de los productos / servicios de la organización:

i. Definir los productos o servicios: en este paso, la máxima autoridad de la organización y el equipo encargado del SIA debería responder la siguiente pregunta: *¿Qué productos y servicios debería continuar brindando la organización tras un evento disruptivo?*

ii. Categorizar y describir las expectativas de las personas beneficiarias de los servicios seleccionados y las posibles sanciones en caso de no entregar los servicios.

iii. Definir el efecto que un evento disruptivo puede ocasionar en las partes interesadas.

iv. Definir los parámetros de tiempo por cada disrupción que establecen los plazos que son determinantes para la continuidad del servicio. A continuación, se describen los parámetros:

1. tiempo objetivo de recuperación (*Recovery Time Objective*, RTO): tiempo que se determina para reactivar una actividad ante la ocurrencia de un evento disruptivo.
2. período máximo de disrupción tolerable (*Maximum Tolerable Period Disruption,* MTPD): tiempo que se determina en el cual la paralización de las actividades es intolerable o inaceptable. También referido como disrupción máxima aceptable (*Maximum Acceptable Outage*, MAO), que corresponde al punto de no retorno con el fin de diseñar las estrategias acordes con estos parámetros.
3. objetivo mínimo de continuidad del servicio (*Minimum Service Continuity Objective*, MSCO): corresponde al nivel mínimo de servicio que se considera aceptable en el momento de la disrupción.
4. objetivo de punto de recuperación (*Recovery Point Objective,* RPO): corresponde al punto en el cual la información utilizada por una actividad se restablece para permitir que la actividad opere al reanudarse.

b. Priorización de procesos:

Priorizado los productos y el alcance del proceso de continuidad que ha marcado la dirección, es necesario establecer el alcance del SIA, para saber hasta dónde llegar, los mapas de procesos y productos que se ofrecen y los requisitos legales, reglamentarias y contractuales.

Al listar todos los procesos y priorizarlos se obtendrán:

- La correlación entre procesos, productos y actividades.
- Identificar las dependencias entre procesos, productos y actividades.
- Poder evaluar el impacto de la paralización de un proceso.
- Listar todos los procesos priorizados que nos ofrecen productos y servicios.
- Listar la interdependencia entre procesos.
- Listar las actividades que forman parte de los procesos.

El planteamiento puede ser visual por medio de un diagrama porque de esta manera se podrán representar las dependencias y todas las actividades relacionadas con el proceso o también con una tabla.

Cuando se tengan todos los procesos listados y ordenados se deben priorizar siguiendo las orientaciones que previamente dio la dirección sobre los productos, para poder trabajar sobre ellos.

c. Priorización de actividades:

Los procesos están formados por actividades que interactúan entre sí para alcanzar uno o varios resultados concretos; lo que procede en ese momento del análisis es examinar las prioridades a nivel de “actividad” e identificar los recursos necesarios que se necesitan para desarrollarse con normalidad. Al conocer este dato se podrá hacer una estimación de los recursos necesarios para la recuperación ante un evento disruptivo.

Se recomienda utilizar fichas de procesos, esto para su caracterización y conocer las actividades o subprocesos que contienen y los recursos necesarios.

La información para obtener estos recursos incluye el detalle de:

- Instalaciones
- Recursos humanos, incluyendo sus habilidades y puestos
- Los registros de documentación
- Suministros
- Recursos financieros
- Las dependencias y relaciones de otros procesos
- Las herramientas
- La normativa que se debe cumplir

Para recopilar esa información de manera ordenada es necesario revisar todas las prioridades de los procesos trabajadas con anterioridad, el organigrama, el mapa de procesos, y todos los documentos necesarios que se han ido generando con el SIA. De cada actividad hay que recopilar los detalles para la priorización y dentro de esto están los procedimientos y tiempos para las actividades, los picos de demandas de los servicios y cualquier otro factor relevante.

En cuanto a los recursos necesarios es importante indicar además de las personas, las materias primas, los equipamientos, detallar si hay actividades subcontratadas y los niveles de suministro mínimos garantizados, los requisitos de los lugares de trabajo, las necesidades de tecnologías de la información y comunicación y otros.

d. Análisis y consolidación:

Las actividades tienen interdependencias entre sí, recursos y cadenas de suministro. Por eso es necesario hacer una mención a las interdependencias internas y externas de estas actividades; el mapa de procesos es muy útil como apoyo para seleccionar estas interdependencias.

Tras este análisis es necesario que la alta jerarquía de la organización respalde el documento de análisis de impacto en el servicio y especialmente las priorizaciones de productos, procesos y actividades. Por ello es necesario que en el informe se recopile la visión total del proceso del SIA, los impactos más importantes que determinan los requisitos y los plazos recomendados. Una vez que se ha terminado este proceso se puede dar un paso más y seleccionar la estrategia de continuidad.

e. Resultado final y respaldo de la alta jerarquía de la organización:

Priorizar actividades sirve para validar la información sobre como el impacto del factor tiempo afecta a las disrupciones. También nos indica qué recursos son necesarios para las actividades prioritarias, las dependencias y los recursos necesarios para estas actividades.

Con toda la documentación e información que se ha ido extrayendo se debería realizar un informe final en el que se revisen las prioridades para tomar buenas decisiones sobre la continuidad de las actividades.

El enfoque del análisis elegido debería ser el apropiado para obtener la mejor información teniendo en cuenta los recursos, los conocimientos y la información de la que se dispone. La información debe ser comprobada, contrastada y revisada para que todo lo que se ha escrito sea coherente.

Este análisis final a partir de toda la información reunida puede combinar técnicas cualitativas y cuantitativas. Al concluir el análisis se busca confirmar que los impactos que se han valorado son correctos y que las dependencias y necesidades de los recursos sean adecuadas.

8.2.3 Evaluación de riesgos

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

Nota. El proceso para la evaluación de riesgos se aborda en la norma INTE/ISO 31000.

La organización pública y sin fines de lucro debe:

a) identificar los riesgos de disrupción para las actividades priorizadas de la organización y de los recursos requeridos;
b) analizar y evaluar los riesgos identificados;
c) determinar cuáles riesgos requieren tratamiento.

Nota. Los riesgos en este apartado se relacionan con la disrupción de las actividades del servicio. Los riesgos y oportunidades relacionados con la efectividad del sistema de gestión se abordan en el apartado 6.1.

El objetivo de realizar una evaluación de riesgo consiste en permitir a la organización determinar la probabilidad de ocurrencia de incidentes, además de 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 periodos planificados o cuando se produzcan cambios significativos en la organización o en el contexto en el que opera. El proceso de evaluación de riesgos debería:

- 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 para la identificación de estrategias.

8.3 Estrategias y soluciones de continuidad del servicio

8.3.1 Generalidades

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

Estas estrategias persiguen proteger las actividades priorizadas y reanudarlas con celeridad en caso de que sean afectadas por un evento disruptivo, mitigar y gestionar el impacto. Lo que se persigue es, entre otras:

- Identificar estrategias para reducir la frecuencia de incidentes disruptivos.
- Identificar que recursos financieros serán necesarios y tenerlos preparados.
- Desarrollar las capacidades de comunicación y tomar medidas para abordar la falta de disponibilidad de personal.
- Planificar medios alternativos para poder seguir desarrollando las actividades prioritarias en caso de pérdida y las capacidades para recuperar la actividad.
- Desarrollar capacidades para recuperar activos de Tecnologías de Información y Comunicación incluyendo los datos que se han perdido.
- Desarrollar medios alternativos de entrega de productos y prestar servicios.

8.3.2 Identificación de estrategias y soluciones.

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

a) cumplan con los requisitos para continuar y recuperar actividades priorizadas dentro de los plazos identificados y la capacidad acordada;
b) protejan las actividades priorizadas de la organización pública y sin fines de lucro;
c) reduzcan la probabilidad de disrupción;
d) acorten el período de disrupción;
e) limiten el impacto de la disrupción en los productos y servicios de la organización;
f) provean la disponibilidad de recursos adecuados.

La identificación de las estrategias adicionalmente debería contar con al menos:

- Un análisis de contexto externo a interno
- Conocer las necesidades y las expectativas de las partes interesadas
- Tener los roles adecuadamente asignados
- Disponer de recursos suficientes
- Haber finalizado el análisis de impacto en el servicio
- Tener finalizada la evaluación del riesgo

La existencia de estos requisitos previos es necesaria para una adecuada identificación de estrategias de continuidad.

8.3.3 Selección de estrategias y soluciones.

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

a) cumplan con los requisitos para continuar y recuperar actividades priorizadas dentro de los plazos identificados y la capacidad acordada;
b) consideren la cantidad y el tipo de riesgo que la organización puede o no asumir;
c) consideren los costos y beneficios asociados.

Posterior a la identificación es necesario el proceso de selección de acuerdo con estrategias preestablecidas, para ello, deben cumplir con el plazo analizado para la recuperación, además considerar el tipo de riesgos y los costos asociados.

Determinar y seleccionar las estrategias, es el proceso mediante el cual se eligen las capacidades que se pueden implementar para mitigar el impacto de los incidentes disruptivos. Se debería tener un mecanismo para aprobar, validar y revisar las estrategias propuestas.

Los principios que conforman la determinación de las estrategias están enfocados a:

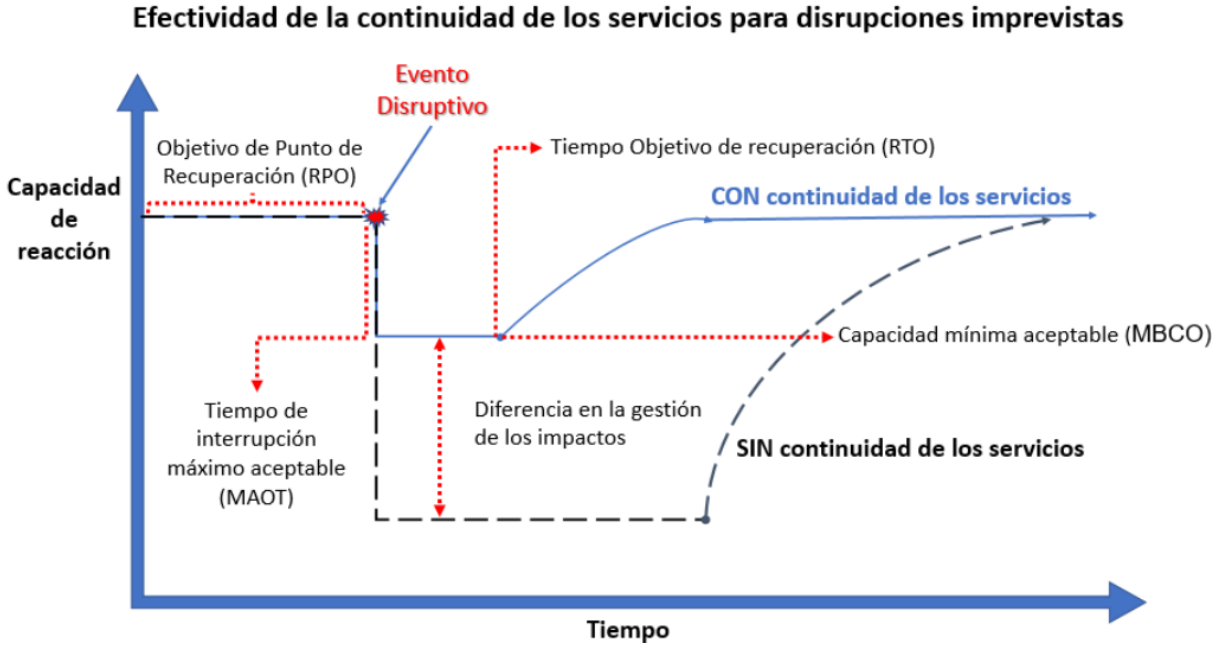
- Proteger las actividades priorizadas frente a una disrupción.
- Estabilizar, continuar, reanudar y recuperar las actividades priorizadas, las dependencias y los recursos que han sufrido una disrupción.

Estas estrategias deben estar basadas en los resultados obtenidos en el SIA y en la evaluación de riesgos, y deben cumplir los requisitos para poder lograr los objetivos de continuidad y concretamente los tiempos objetivos de recuperación (RTO), objetivo de punto de recuperación (RPO) y los niveles de servicio. En general, cuando mayor sea la prioridad, es decir que el RTO sea más corto, la recuperación es más compleja y costosa.

Se recomienda algunos puntos para la selección de las estrategias:

- Si las organizaciones deciden o no actuar, y actuar de manera reactiva, llegado el momento debería hacerse con base en unos criterios predefinidos. Esta estrategia se puede usar cuando el tiempo para recuperarse es suficiente. Si la decisión de no actuar es consecuencia de que no se ha hecho una implementación, no sería aceptable.
- El contexto del servicio toma relevancia a la hora de determinar qué estrategias son aplicables. No es lo mismo trabajar en un entorno donde hay multas y sanciones establecidas por interrupciones que en un entorno libre de estas penalizaciones.
- En un entorno altamente competitivo puede que tampoco sea recomendable la subcontratación por el potencial abandono de clientes al conocer a un nuevo proveedor.
- Si se opta por recursos alternativos, debería tenerse en cuenta la distancia a la que se encuentra, por ejemplo, si existe una caída del fluido eléctrico generalizada o una avería, el mismo evento puede afectar a dos instalaciones que geográficamente estén muy cerca.
- La ubicación geográfica de recursos alternativos debería establecerse teniendo en cuenta al menos: el clima, la estabilidad geológica, la estabilidad política y la infraestructura, entre otros.
- Se debería tener en cuenta variables como la eficacia del recurso, la relación costo beneficio y el contexto donde se va a implementar, las debilidades de los proveedores de los que se va a depender y que existan los recursos suficientes, entre otros.

En la siguiente figura se presentan algunas de las variables que inciden en la eficacia de la operación de la organización con un sistema de gestión de continuidad del servicio o sin él.



Fuente: Adaptada de la norma INTE/ISO 22313

Figura 5. Efectividad de la continuidad de los servicios para disrupciones

8.4 Planes y procedimientos de continuidad del servicio

8.4.1 Generalidades

La organización pública y sin fines de lucro debe implementar y mantener una estructura de respuesta que permita una advertencia (alerta) oportuna y comunicación pertinente a las partes interesadas. Debe proporcionar planes y procedimientos para gestionar la organización durante una disrupción; estos se deben utilizar cuando sea necesario para activar soluciones de continuidad del servicio.

Nota. Existen diferentes tipos de procedimientos que comprenden planes de continuidad del servicio.

La organización pública y sin fines de lucro debe identificar y documentar los planes y procedimientos de continuidad del servicio basados en las estrategias y las soluciones seleccionadas. Los procedimientos deben:

a) ser específicos con respecto a los pasos inmediatos que se deben tomar durante una disrupción;
b) ser flexibles para responder a las condiciones cambiantes internas y externas de una disrupción;
c) centrarse en el impacto de los incidentes que potencialmente conducen a la disrupción;
d) ser eficaces para minimizar el impacto mediante la implementación de soluciones apropiadas;
e) asignar roles y responsabilidades para tareas dentro de ellos.

Para que las estrategias seleccionadas sean eficaces y aseguren que se activan llegado el momento, es conveniente que los planes de respuesta dispongan de acciones y procedimientos claros. De esta manera cada actor sabrá las acciones que tiene que realizar para su plan de continuidad.

Estos procedimientos deberían ser específicos indicando cada acción a realizar a los roles asignados, pero lo suficientemente flexibles para poder adaptarse a cambios en las condiciones de un evento disruptivo. Los equipos responsables de la implementación deberían:

- Estar preparados y dotados de la autoridad necesaria para activar dichos planes.

- Contar con los recursos necesarios para comunicar interna y externamente la activación del plan y tener por escrito los planes de continuidad para poder orientar y servir de apoyo en la respuesta y recuperación.
- Documentar los planes de continuidad para orientar a los equipos sobre qué se debe hacer para proseguir y recuperar las actividades prioritarias, saber en qué momento deben activarse y los procedimientos para que las entregas de servicios se realicen de acuerdo con una capacidad previamente definida.
- Cada uno de estos planes deberían indicar sus objetivos, los responsables de este, las acciones que se deben realizar, los recursos necesarios y en qué momento y bajo que umbrales dejan de ser necesarios.

8.4.2 Estructura de respuesta

8.4.2.1 La organización pública y sin fines de lucro debe implementar y mantener una estructura, identificando uno o más equipos responsables de responder a las disrupciones.

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

8.4.2.3 Colectivamente, los equipos deben ser competentes para:

a) evaluar la naturaleza y el alcance de una disrupción y su impacto potencial;
b) evaluar el impacto contra umbrales predefinidos que justifican el inicio de una respuesta formal;
c) activar una respuesta adecuada de continuidad del servicio;
d) planificar acciones que deben llevarse a cabo;
e) establecer prioridades (considerando como primera prioridad salvaguardar la vida);
f) monitorear los efectos de la disrupción y la respuesta de la organización;
g) activar las soluciones de continuidad del servicio;
h) comunicarse con las partes interesadas pertinentes, las autoridades y los medios de comunicación.

8.4.2.4 Para cada equipo debe existir:

a) personal identificado y sus suplentes con la responsabilidad, autoridad y competencia para desempeñar su papel designado;
b) procedimientos documentados para guiar sus acciones (ver apartado 8.4.4), incluidos los de activación, operación, coordinación y comunicación de la respuesta.

La experiencia y la práctica actúan como mitigadores ante cualquier tipo de riesgo. Es necesario que la organización sepa la forma en la que debería actuar en cada caso, esto permite que se reaccione de mejor manera frente a situaciones nuevas.

Cuando se habla de riesgos y de eventos bajo incertidumbre es frecuente que se tengan que afrontar situaciones nuevas. Por eso es importante realizar ejercicios prácticos y simulacros ante eventos disruptivos. Además de haber ensayado los pasos permite aplicar una mejora continua en los ejercicios detectando fallos e ineficiencias.

8.4.3 Advertencia (alertamiento) y comunicación

8.4.3.1 La organización pública o sin fines de lucro debe documentar y mantener procedimientos para:

a) comunicarse interna y externamente con las partes interesadas pertinentes, incluyendo qué, cuándo, con quién y cómo comunicarse;

Nota. La organización pública o sin fines de lucro puede documentar y mantener procedimientos sobre cómo y bajo qué circunstancias, la organización se comunica con los empleados y sus contactos de emergencia.

b) recibir, documentar y responder a las comunicaciones de las partes interesadas, incluido cualquier sistema de asesoramiento de riesgos nacional o regional o equivalente;
c) asegurar la disponibilidad de los medios de comunicación durante una disrupción;
d) facilitar la comunicación estructurada con el equipo de respuesta de emergencias;
e) proporcionar detalles de la respuesta de los medios de la organización después de un incidente, incluida una estrategia de comunicaciones;
f) registrar los detalles de la disrupción, las acciones y las decisiones tomadas.

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

a) alertar a las partes interesadas potencialmente afectadas por una disrupción real o inminente;
b) asegurar una coordinación y comunicación apropiadas entre las múltiples organizaciones que responden.

Los procedimientos de advertencia y comunicación se deben ejercer como parte del ejercicio de la organización, programa descrito en el apartado 8.5.

En la comunicación interna y externa de la organización pública o sin fines de lucro, se pueden incluir partes interesadas como los colaboradores, proveedores, contactos de emergencia, junta directiva, direcciones, gerencia, clientes, entre otros; a los que la organización decide qué tipo de comunicación realizar para cada uno.

8.4.4 Planes de continuidad del servicio

8.4.4.1 La organización debe documentar y mantener los planes y procedimientos de continuidad del servicio, estos deben proporcionar orientación e información para ayudar a los equipos a responder a una disrupción y para ayudar a la organización con respuesta y recuperación.

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

a) detalles de las acciones que tomarán los equipos para:
1) continuar o recuperar actividades priorizadas dentro de marcos de tiempo predeterminados;
2) dar seguimiento al impacto de la disrupción y la respuesta de la organización a ella;
b) referencia a los umbrales predefinidos y al proceso para activar la respuesta;
c) procedimientos para permitir la entrega de productos y servicios a la capacidad acordada;
d) detalles para gestionar las consecuencias inmediatas de una disrupción teniendo debidamente en cuenta:
1) el bienestar de las personas;
2) la prevención de nuevas pérdidas o falta de disponibilidad de actividades priorizadas;
3) el impacto en el ambiente.

8.4.4.3 Cada plan debe incluir:

a) el propósito, alcance y objetivos;
b) los roles y responsabilidades del equipo que implementará el plan;
c) acciones para implementar las soluciones;

d) información de apoyo necesaria para activar (incluidos los criterios de activación), operar, coordinar y comunicar las acciones del equipo;
e) interdependencias internas y externas;
f) los requisitos de recursos;
g) los requisitos de presentación de informes;
h) un proceso para suspender operaciones.

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

8.4.5 Recuperación

La organización pública y sin fines de lucro debe tener procesos documentados para recuperar y restaurar las actividades del servicio con medidas temporales adoptadas durante y después de una disrupción.

Como todo proceso adicional en el SGCS, es necesario contar con información que respalde la fase de recuperación posterior a una disrupción. Para ello se recomienda que se cuente con un procedimiento de evaluación posterior al incidente, esto con el objetivo de las acciones para la mejora continua y permita el autoconocimiento e identificar las lecciones aprendidas.

8.5 Programa de ejercicios

La organización pública y sin fines de lucro debe implementar y mantener un programa de ejercicios y pruebas para validar la efectividad de sus estrategias y soluciones de continuidad del servicio. La organización debe realizar ejercicios y pruebas que:

a) sean consistentes con sus objetivos de continuidad del servicio;
b) se basen en escenarios apropiados que están bien planificados con metas y objetivos claramente definidos;
c) desarrollen el trabajo en equipo, la competencia, confianza y el conocimiento para aquellos que tienen roles que desempeñar en relación con las disrupciones;
d) en conjunto, a lo largo del tiempo, validen sus estrategias y soluciones de continuidad del servicio;
e) produzcan informes formales posteriores al ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras;
f) se revisen en el contexto de la promoción de la mejora continua;
g) se realicen a intervalos planificados y cuando hay cambios significativos dentro de la organización o el contexto en el que opera.

La organización debe actuar sobre los resultados de su ejercicio y prueba para implementar cambios y mejoras.

Basado en lo anterior, es necesario que la organización realice ejercicios prácticos y simulacros relacionados con eventos disruptivos. Además de haber ensayado los pasos, ello permite aplicar una mejora continua en los ejercicios, detectando fallos e ineficiencias.

8.6. Evaluación de la documentación y las capacidades de continuidad del servicio

La organización pública y sin fines de lucro debe:

a) evaluar la idoneidad, adecuación y efectividad de su análisis de impacto en el servicio, evaluación de riesgos, estrategias, soluciones, planes y procedimientos;
b) realizar evaluaciones a través de revisiones, análisis, ejercicios, pruebas, informes posteriores al incidente y evaluaciones de desempeño;
c) realizar evaluaciones de las capacidades de continuidad del servicio de socios y proveedores pertinentes;
d) evaluar el cumplimiento de los requisitos legales y reglamentarios aplicables, las mejores prácticas de la industria, y conformidad con su propia política y objetivos de continuidad del servicio;
e) actualizar la documentación y los procedimientos de manera oportuna.

Estas evaluaciones se deben llevar a cabo a intervalos planificados, después de un incidente o activación, y cuando se producen cambios significativos.

Dentro del esquema de mejora continua es necesario que se realice un seguimiento de todo el SGCS para medir, analizar y asegurar los resultados pretendidos, para ello es necesario designar a los responsables de hacer este seguimiento.

Si el plan de continuidad se elabora dentro de un SGCS, como este es auditable, se debe documentar todo el sistema para que pueda ser revisado internamente y poder evaluar si los requisitos y dicho sistema, cumplen con las exigencias de esta norma, debiendo realizar las mejoras necesarias cuando se presenten no conformidades.

9 EVALUACIÓN DE DESEMPEÑO

9.1 Seguimiento, medición, análisis y evaluación

La organización pública y sin fines de lucro debe determinar:

a) a qué se le debe dar seguimiento y medición;
b) los métodos de seguimiento, medición, análisis y evaluación, según corresponda, para asegurar la validez de los resultados;
c) cuándo y quién debe realizar el seguimiento y la medición;
d) cuándo y por quién se deben analizar y evaluar los resultados del seguimiento y la medición.

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

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

9.2 Auditoría interna

9.2.1 Generalidades

La organización pública y sin fines de lucro debe realizar auditorías internas a intervalos planificados para proporcionar información sobre si el SGCS:

a) se ajusta a:
1) los requisitos propios de la organización para su SGCS;
2) los requisitos de este documento;
b) se implementa y mantiene de manera efectiva.

9.2.2 Programas de auditoría

La organización pública y sin fines de lucro debe:

a) planificar, establecer, implementar y mantener un programa de auditoría que incluya la frecuencia, los métodos, responsabilidades, requisitos de planificación e informes, que deben tener en cuenta la importancia de los procesos en cuestión y los resultados de auditorías anteriores;
b) definir los criterios de auditoría y el alcance de cada auditoría;
c) seleccionar auditores y realizar auditorías para asegurar la objetividad y la imparcialidad del proceso de auditoría;
d) asegurar que los resultados de las auditorías se informan a los gerentes pertinentes;
e) conservar información documentada como evidencia de la implementación de los programas y los resultados de la auditoría;
f) asegurar que se toman las medidas correctivas necesarias sin demora indebida para eliminar las no conformidades detectadas y sus causas;
g) asegurar que las acciones de seguimiento de auditoría incluyan la verificación de las acciones tomadas y el informe de resultados de verificación.

9.3 Revisión por la dirección

9.3.1 Generalidades

La alta dirección debe revisar el SGCS de la organización pública y sin fines de lucro, a intervalos planificados, para asegurar su continua idoneidad, adecuación y efectividad.

9.3.2 Aporte de la revisión por la dirección

La revisión por la dirección debe considerar:

a) el estado de las acciones de revisiones previas por la dirección;
b) cambios en aspectos externos e internos que son pertinentes para el SGCS;
c) información sobre el desempeño del SGCS, incluyendo las tendencias en:
1) no conformidades y acciones correctivas;
2) resultados de evaluación del seguimiento y medición;
3) resultados de la auditoría;
d) realimentación de las partes interesadas;
e) la necesidad de cambios en el SGCS, incluyendo la política y los objetivos;
f) procedimientos y recursos que podrían usarse en la organización para mejorar el desempeño y efectividad del SGCS;
g) información del análisis de impacto en el servicio y evaluación de riesgos;
h) resultado de la evaluación de la documentación y de las capacidades de continuidad del servicio (ver apartado 8.6);
i) riesgos o problemas no abordados adecuadamente en cualquier evaluación de riesgos previa;
j) lecciones aprendidas y acciones derivadas de cuasi-accidentes y eventos disruptivos;
k) oportunidades para la mejora continua.

9.3.3 Salidas de la revisión por la dirección

9.3.3.1 Las salidas de la revisión por la dirección deben incluir decisiones relacionadas con la mejora continua, oportunidades y cualquier necesidad de cambios en el SGCS para mejorar su eficiencia y efectividad, incluyendo lo siguiente:

a) variaciones en el alcance del SGCS;
b) actualización del análisis de impacto en el servicio, evaluación de riesgos, estrategias, planes y soluciones de continuidad del servicio;
c) modificación de procedimientos y controles para responder a problemas internos o externos que pueden afectar el SGCS;
d) cómo se medirá la efectividad de los controles.

9.3.3.2 La organización pública y sin fines de lucro debe conservar información documentada como evidencia de las salidas de la revisión por la dirección, para lo cual debe:

a) comunicar las salidas de la revisión por la dirección a las partes interesadas pertinentes;
b) tomar las medidas apropiadas en relación con esos resultados.

10 MEJORA

10.1 No conformidades y acciones correctivas

10.1.1 La organización pública o sin fines de lucro debe determinar oportunidades de mejora e implementar las acciones necesarias para lograr los resultados previstos de su SGCS.

10.1.2 Cuando ocurre una no-conformidad, la organización debe:

a) reaccionar ante la no conformidad y, según corresponda:
1) tomar medidas para controlarla y corregirla;
2) lidiar con las consecuencias;
b) evaluar la necesidad de actuar para eliminar la(s) causa(s) de la no conformidad, a fin de que no vuelva a ocurrir ni ocurra en otra parte, al:
1) revisar la no conformidad;
2) determinar las causas de la no conformidad;
3) determinar si existen no conformidades similares, o si pueden ocurrir potencialmente;
c) implementar cualquier acción necesaria;
d) revisar la efectividad de cualquier acción correctiva tomada;
e) aplicar cambios en el SGCS, si es necesario.

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

10.1.3 La organización pública o sin fines de lucro debe conservar información documentada como evidencia de:

a) la naturaleza de las no conformidades y cualquier acción posterior tomada al respecto;
b) los resultados de cualquier acción correctiva.

11 MEJORA CONTINUA

La organización pública o sin fines de lucro debe mejorar continuamente la idoneidad, adecuación y efectividad del SGCS, con base en medidas cualitativas y cuantitativas.
La organización debe considerar los resultados del análisis y la evaluación, y las salidas de la revisión por la dirección, para determinar si hay necesidades u oportunidades, relacionadas con el servicio, o con el SGCS, que se deben abordar como parte de la mejora continua.

Nota. La organización puede utilizar los procesos del SGCS, como liderazgo, planificación y evaluación desempeño, para lograr la mejora.

12 CORRESPONDENCIA

Esta norma nacional no es equivalente (NEQ) con ninguna norma internacional, por no existir referencia alguna al momento de su elaboración.

Para el desarrollo de esta norma se toma como base la norma ISO 22301:2019 “Security and resilience — Business continuity management systems — Requirements”.

BIBLIOGRAFÍA

[1] ISO 9001, *Quality management systems — Requirements*

[2] ISO 14001, *Environmental management systems — Requirements with guidance for use*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO/IEC/TS 17021-6, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 6: Competence requirements for auditing and certification of business continuity management systems*

[5] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[6] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[7] ISO 22316, *Security and resilience — Organizational resilience — Principles and attributes*

[8] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*

[9] ISO/TS 22318, *Societal security — Business continuity management systems — Guidelines for supply chain continuity*

[10] ISO/TS 22330, *Security and resilience — Business continuity management systems — Guidelines for people aspects of business continuity*

[11] ISO/TS 22331, *Security and resilience — Business continuity management systems — Guidelines for business continuity strategy*

[12] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

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

[14] ISO 28000, *Specification for security management systems for the supply chain*

[15] ISO 31000, *Risk management — Guidelines*

[16] IEC 31010, *Risk management — Risk assessment techniques*

[17] ISO Guide 73, *Risk management — Vocabulary*

[18] CGR. (2020). Gestión de la continuidad institucional. Recuperado de https://sites.google.com/cgr.go.cr/covid-19/Continuidad-servicios-publicos/Gestion-de-la-continuidad-eje-1

[19] Asamblea Legislativa. (2008). Ley de la Autoridad Reguladora de Servicios Públicos Nº7593 artículo 3.

[20] Ministerio de Planificación y Política Económica. (2016). Marco conceptual y estratégico para el fortalecimiento de la Gestión para Resultados en el Desarrollo en Costa Rica.

[21] Asamblea Legislativa. (2002). Ley General de Control Interno Nº8292 artículo 2.

ANEXO A (INFORMATIVO)

FAMILIA DE NORMAS DE ORIENTACIÓN DE CONTINUIDAD DEL SERVICIO

Existen un conjunto de normas desarrolladas por la Organización Internacional de Normalización (ISO), que proporcionan un marco de gestión para la continuidad del servicio alineados con los objetivos de servicio, y optimizando las inversiones realizadas en controles o salvaguardas que protejan los activos. Dicho conjunto de normas se resume en la familia INTE/ISO 22300: relacionada con directrices, marco y vocabulario sobre continuidad del negocio. La familia de normas INTE/ISO27000: enfocadas en conceptos y principios sobre tecnología ante eventos disruptivos. Por último, la familia INTE/ISO31000: relacionadas con la gestión del riesgo. Esta familia de normas es incluida como una guía de referencia. En la siguiente imagen se presenta un resumen de las principales normas alineadas:

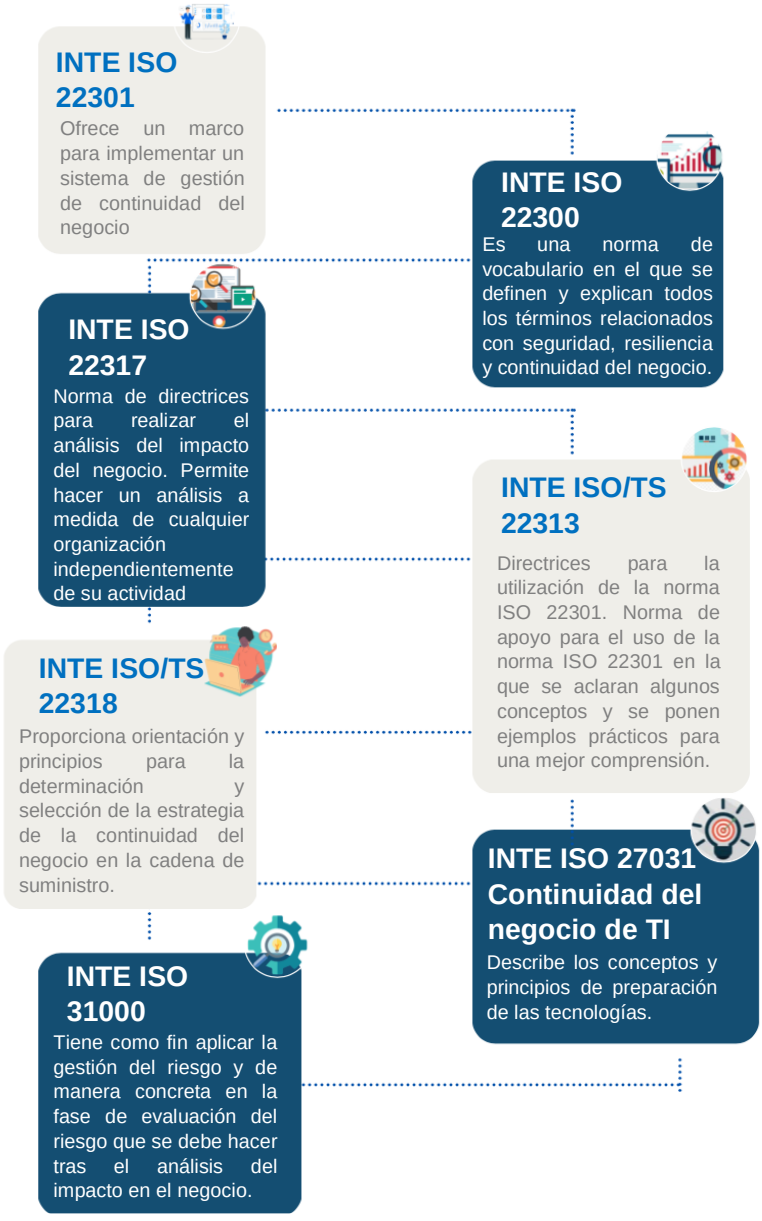


Figura 6 — Familia de Normas de orientación sobre continuidad del negocio

ANEXO B(INFORMATIVO)

MARCO NORMATIVO SOBRE CONTINUIDAD DEL SERVICIO

La continuidad del servicio a nivel de sector público se encuentra normado por medio de la legislación vigente. En la siguiente tabla se mencionan las principales leyes y documentos aplicables a las temáticas, así como normativa de referencia como lo son las normas ISO.

Tabla B.1 — Resumen del marco normativo sobre continuidad del servicio

Documento / Norma	Descripción
NORMATIVA APLICABLE AL SECTOR PÚBLICO	
Ley General de Administración Pública Nº 6227 Art. 4	Establece que la actividad de los entes públicos deberá estar sujeta en su conjunto a los principios fundamentales del servicio público, para asegurar su **continuidad**, su eficiencia, su adaptación a todo cambio en el régimen legal o en la necesidad social que satisfacen y la igualdad en el trato de los destinatarios, usuarios o beneficiarios. Link: http://www.pgrweb.go.cr/SCIJ/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=13231
Ley Nacional de Emergencias y Prevención del Riesgo Nº8488	La finalidad de estas normas es conferir un marco jurídico ágil y eficaz, que garantice la reducción de las causas del riesgo, así como el manejo oportuno, coordinado y eficiente de las situaciones de emergencia. Link: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=56178
Ley General de Control Interno Nº 8292	Esta Ley establece los criterios mínimos que deberán observar la Contraloría General de la República y los entes u órganos sujetos a su fiscalización, en el establecimiento, funcionamiento, mantenimiento, perfeccionamiento y evaluación de sus sistemas de control interno. El control interno cuenta con los siguientes objetivos: a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal. b) Exigir confiabilidad y oportunidad de la información. c) Garantizar eficiencia y eficacia de las operaciones. d) Cumplir con el ordenamiento jurídico y técnico. Link: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=49185&nValor3=52569
Ley de la Autoridad Reguladora de los Servicios Públicos (ARESEP) Nº 7593	Define el concepto de servicio público: Es un servicio que por su importancia para el desarrollo sostenible del país es calificado como tal por la Asamblea Legislativa, con el fin de sujetarlo a las regulaciones de esta ley (Ley N° 7593, 1996, art. 3). Son los bienes o servicios que no pueden ser disfrutados por un individuo sin que otros tengan acceso a ellos. El disfrute del servicio público es general, y para toda la población. Link: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=26314
Política Nacional de Gestión del Riesgo 2016-2030	Establece que en la función pública es necesaria una continuidad de los servicios públicos y no sólo la protección o recuperación de las obras, aspecto que resulta importante en un enfoque de recuperación económica y social.

Documento / Norma	Descripción
NORMATIVA APLICABLE AL SECTOR PÚBLICO	
	Link: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=80654&nValor3=102417#:~:text=El%20objetivo%20de%20desarrollo%20de%20la%20Pol%C3%ADtica%20Nacional,recuperaci%C3%B3n%20efectiva%20ante%20los%20posibles%20eventos%20de%20desastre.
Plan Nacional de Gestión del Riesgo 2021- 2025	Se establece como reto institucional adoptar políticas de continuidad del servicio en el sector público, lo cual implica aprendizaje y labor compartida con el sector privado. Desde el Sistema Nacional de Gestión del Riesgo, cabe la alternativa de crear instancias de coordinación para articular estos esfuerzos. Link: https://www.cne.go.cr/rectoria/planngr/Plan%20Nacional%20de%20Gestion%20del%20Riesgos%202021-2025.pdf
Estudio de la Gestión y estado de la continuidad de los servicios públicos en la emergencia	Producto de la pandemia por COVID-19, la Contraloría General de la República determina el nivel de gestión de la continuidad de 21 servicios públicos críticos, con base en el análisis de buenas prácticas aplicadas por las 90 instituciones públicas a cargo de su prestación; así como, el estado de dichos servicios. Esto con el propósito de promover la aplicación de prácticas preventivas y correctivas para su prestación continua en procura de salvaguardar los derechos y el bienestar de la ciudadanía.
Lineamientos de Continuidad de los Servicios	Corresponden a un grupo de lineamientos desarrollados en el contexto de la pandemia por COVID-19 con el objetivo de orientar a los sectores productivos para continuar brindando los servicios a un nivel mínimo aceptable.
Normas técnicas para la gestión y el control de las Tecnologías de Información	Continuidad y disponibilidad operativa de los servicios tecnológicos. La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas. Lin: https://www.micitt.go.cr/wp-content/uploads/2022/05/Normas-Micitt-Normas-te%CC%81cnicas-para-el-gobierno-y-gestio%CC%81n-de-las-tecnologi%CC%81as-de-la-informacio%CC%81n-2021.pdf
PRINCIPALES NORMAS INTE/ISO VIGENTES	
INTE/ISO 31000	Gestión del riesgo. Principios y directrices. Nos ayuda a aplicar la gestión del riesgo y de manera concreta en la fase de evaluación del riesgo que se debe hacer tras el análisis de impacto en el servicio.
INTE/ISO 22300	Es una norma de vocabulario en el que se definen y explican todos los términos relacionados con seguridad, resiliencia y continuidad del servicio.

Documento / Norma	Descripción
NORMATIVA APLICABLE AL SECTOR PÚBLICO	
INTE/ISO 22301	Ofrece un marco para implementar un sistema de gestión de continuidad de servicios. Además, tiene el apoyo de otras normas de la misma familia para profundizar y guiar en la implementación de este sistema. Su estructura de sistema de gestión permite que se implemente teniendo en cuenta los criterios de alto nivel de ISO dictados por el Anexo SL lo que permite, además de su mejora continua, que sea auditable.
INTE/ISO 22317	Es una norma de directrices para realizar el análisis de impacto de servicio. Al tratarse de una norma de principios y directrices nos permite hacer un análisis a medida de cualquier organización independientemente de su actividad.
INTE ISO/TS 22313	Directrices para la utilización de la norma ISO 22301. Es una norma de apoyo para el uso de la norma ISO 22301 en la que se aclaran algunos conceptos y se ponen ejemplos prácticos para una mejor comprensión.
INTE ISO/TS 22331	Directrices para la estrategia de continuidad del servicio.
INTE/ISO/TS 22318	Proporciona orientación y principios para la determinación y selección de la estrategia de continuidad del servicio en la cadena de suministro.
ISO 27031 Continuidad de servicio TI	Describe los conceptos y principios de la preparación de las tecnologías de información y comunicación (TIC) para la continuidad del servicio, y proporciona un marco de referencia de métodos y procesos para identificar y especificar todos los aspectos (tales como los criterios de desempeño, diseño e implementación) para la mejora en la preparación de las TIC de la organización para asegurar la continuidad del servicio.

ANEXO C (INFORMATIVO)

REQUISITOS PREVIOS PARA ANÁLISIS DE IMPACTO DEL SERVICIO

En la siguiente tabla se menciona un resumen de los requisitos previos para la realización de un Análisis de Impacto del Servicio.

Tabla C.1 — Resumen de los requisitos previos a la realización de un Análisis de Impacto del Servicio

Requisitos	Descripción	Preguntas orientadoras
1. Definición del contexto 	Consiste en conocer el contexto interno y externo de la organización y en el que se deben entregar los productos o servicios. Una de las técnicas recomendadas para la determinación del contexto es el análisis PESTEL o análisis FODA.	**A nivel de contexto interno:** **Estrategia:** 1.1 ¿Cuáles son los objetivos, misión y visión de la organización? **Procesos y servicios:** 1.2 ¿Cuáles son los principales procesos de la organización? Enumere los servicios que presentan mayor demanda. **Desempeño:** 1.3 ¿Cuál es el nivel de desempeño de la organización? **Satisfacción:** 1.4 ¿Cuáles son los principales resultados de la satisfacción de las partes interesadas? **Marco Normativo:** 1.5 ¿Cuál es el Marco Normativo (leyes, decretos, reglamentos, de la organización)? **Recursos disponibles:** 1.6 Descripción de los recursos disponibles en la organización: presupuesto, recursos humanos, tecnológicos entre otros. **A nivel de contexto externo:** **Afectación de partes interesadas:** 1.7 ¿Cuáles son las partes interesadas que pueden verse afectadas ante la interrupción de los servicios? ¿Qué impacto tendría en cada uno? 1.8 ¿Cuál es el mecanismo que asegura que las partes interesadas se encuentran comprometidas y con un mandato adecuado? **Cumplimiento de partes interesadas (proveedores):** 1.9 ¿Las partes interesadas externas cumplen sus compromisos a tiempo (proveedores)?

Requisitos	Descripción	Preguntas orientadoras
		Normativa aplicable: 1.10 ¿Cuál es la normativa que se debe considerar para la aplicación de un Sistema de Gestión en Continuidad del Servicio? ¿Existe alguna obligatoriedad para informar a alguna institución reglamentaria que se cuenta con un Sistema de Continuidad del Servicio? **Entorno económico:** 1.11 ¿Cómo afecta el entorno económico (políticas monetarias, impuestos, tipo de cambio, tendencias económicas, entre otros) a la organización? **Entorno político:** 1.12 ¿Cómo afecta el entorno político (políticas gubernamentales, tratados comerciales, programas de financiamiento entre otros) a la organización? **Entorno ambiental:** 1.13 ¿Existen políticas medioambientales que influyen en el Sistema de Continuidad del Servicio de la organización? **Capacidad de respuesta:** 1.14 ¿Cuáles son las organizaciones o entidades a nivel del sector público, tercer sector o sector privado que requeriría para responder ante un evento disruptivo (ejemplo infraestructura, equipos, servicios de tecnologías de información, suministros, servicios de energía y agua potable)?
2. Definición del alcance	Consiste en definir el alcance del proceso de continuidad del servicio y la interrupción de entrega de qué servicios y productos se pretende analizar. Dependiendo del nivel de avance de la organización con respecto al tema, se puede iniciar de forma parcial y trabajar solo sobre un producto o servicio para posteriormente ir ampliando. Si se decide implementar en toda la organización se deberá priorizar todos los productos y actividades para cada una de las fases de líneas y productos. Esto se puede organizar con uno o varios Análisis de Impacto del	**Cobertura** 2.1 ¿Se requiere aplicar en toda la organización o en qué productos o servicios en específico?

Requisitos	Descripción	Preguntas orientadoras
	Servicio, en función de cómo se decida organizar el proyecto.	
3. Comunicación de responsabili-dades 	Consiste en definir los roles y responsabilidades del proceso.	**Definición de roles:** 3.1 ¿Cuáles son los roles definidos en el proceso? 3.2 ¿Quiénes son los responsables? 3.3 ¿Cuáles son los mecanismos para informar los roles y las responsabilidades en el proceso? 3.4 ¿De qué forma y en qué periodos se informará sobre el desempeño?
4. Compromiso de la máxima autoridad de la organización 	Al ser un nuevo proceso es necesario contar con el compromiso de la máxima autoridad de la organización. En ese sentido se recomienda obtener el compromiso por escrito que respalde la creación del proceso con sustento para la toma de decisiones.	**Compromiso:** 4.1 ¿La máxima autoridad se preocupa por la capacidad de su organización para responder a un incidente disruptivo? 4.2 ¿Cuál es el mecanismo que establece el compromiso de la máxima dirección de la organización con el proceso de continuidad del servicio? 4.3 ¿Las personas representantes de la máxima autoridad de la organización que participen en el proceso tienen suficiente autoridad para la toma de decisiones?
5. Asignar los recursos necesarios 	Consiste en la definición y la asignación de los recursos que la organización dispone para el Sistema de Continuidad del Servicio.	**Disponibilidad de recursos:** 5.1 ¿Cuáles son los recursos necesarios para la ejecución del proceso de continuidad del servicio?