Commented [AES1]: Para saber cómo completar este documento, y ver ejemplos reales de lo que necesita escribir, vea este tutorial en vídeo: "How to Write Business Continuity Strategy According to ISO 22301".

Para acceder al tutorial: en su bandeja de entrada, busque el correo electrónico que recibió en el momento de la compra. Allí, verá un enlace y una contraseña que le permitirán acceder al tutorial en vídeo.

[logo de la organización]

Commented [AES2]: Se deben completar todos los campos de este documento que estén marcados con corchetes [ ].

[nombre de la organización]

ESTRATEGIA DE CONTINUIDAD DE NEGOCIO

Commented [AES3]: Conozca más acerca de la estrategia de continuidad de negocio aquí:

¿Puede ahorrar dinero con una estrategia de continuidad del negocio?
https://advisera.com/27001academy/es/blog/2010/04/02/puede-ahorrar-dinero-con-una-estrategia-de-continuidad-del-negocio/

Código:	
Versión:	
Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Commented [AES4]: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización. En el caso que no exista ese sistema, se puede eliminar esta línea.

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
	0.1	Advisera	Descripción básica del documento

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir qué opciones y decisiones [nombre de la organización] garantizará que se cumplan todas las condiciones para reanudar las actividades comerciales ante el caso de un desastre u otro incidente disruptivo. Constituye la base para preparar el Plan de continuidad de negocio y los planes de recuperación.

Este documento se aplica a todo el alcance del SGCN, según se define en la Política de la gestión de continuidad de negocio.

Los usuarios de este documento son miembros de la alta dirección y personas que implementan el proyecto de gestión de la continuidad de negocio.

Commented [AES5]: Incluya el nombre de su organización.

2. Documentos de referencia

- Norma ISO 22301, cláusulas 8.3 y 8.4.2
- Norma ISO 27001, cláusulas A.5.5 y A.5.29
- Política de continuidad de negocio
- Cuestionarios sobre el análisis de impacto en el negocio
- [Documento de evaluación de riesgos]
- [Documento de tratamiento de riesgos]
- Plan de continuidad de negocio que contiene el Plan de respuesta a los incidentes y los planes de recuperación.

3. Datos de la estrategia

Esta Estrategia y las soluciones relacionadas están redactadas en base a los resultados del Análisis del impacto en el negocio y de la evaluación y tratamiento del riesgo.

Commented [AES6]: Las soluciones se refieren a respuestas

3.1. Análisis del impacto en el negocio

El Análisis del impacto en el negocio establece que [especificar cuántas] actividades sostienen a los productos y servicios clave (consultar el Apéndice 1 – Objetivos de tiempo de recuperación para actividades para obtener una lista de esas actividades).

Commented [AES7]: Incluya aquí el número de actividades que

Commented [AES8]: Para obtener más información sobre este tema, lea este artículo:

3.2. Gestión de riesgos

La evaluación de riesgos que pueden afectar la continuidad de negocio se detalla en [nombre del documento]. Los mayores riesgos que podrían producir un incidente disruptivo, es decir, una interrupción de negocio identificada durante la evaluación de riesgos, son los siguientes:

- [riesgo]

Para todos los riesgos / incidentes mencionados es necesario:

- Aplicar acciones preventivas para reducir la probabilidad de tales incidentes (las acciones se detallan en [nombre del documento]).
- Aplicar acciones preventivas para minimizar las posibles consecuencias de tales incidentes (estas acciones también se detallan en [nombre del documento]).
- Preparar escenarios de eventos que describan cómo esos incidentes afectarían el funcionamiento de la organización (los escenarios están detallados en el Apéndice 1 de esta Estrategia y deben ser utilizados más adelante para los planes de prueba y verificación).
- Definir en el Plan de respuesta a los incidentes la forma adecuada para responder a cada uno de los incidentes.

El [cargo] es el responsable de la redacción de las acciones preventivas y el [cargo] es el responsable de confeccionar el Plan de respuesta a los incidentes.

4. Estructura de respuesta a los incidentes

4.1. Gabinete de crisis y Gabinete de apoyo de crisis

4.1.1. Gabinete de crisis

Si se activan los planes de continuidad de negocio, se conforma un organismo operativo denominado Gabinete de crisis, que está autorizado a tomar las decisiones necesarias para resolver la situación. Los miembros del Gabinete de crisis son:

- [todos los miembros de la alta dirección]
- [persona del departamento de relaciones públicas]
- [persona del departamento de recursos humanos]
- [persona a cargo de adquisiciones, asuntos generales, etc.]
- [coordinador de continuidad de negocio]

El Gabinete de crisis está dirigido por el gerente de crisis. El [cargo] cumplirá un rol de gerente de crisis; en caso de estar ausente, un rol será realizada por el [cargo].

El Gabinete de crisis gestiona el incidente disruptivo desde una instalación denominada Centro de crisis, cuya ubicación se especifica en el punto 5.1 de esta Estrategia.

4.1.2. Gabinete de apoyo de crisis

Commented [AES9]: Para comprender la diferencia entre el

Commented [AES10]: Incluya el nombre del documento de

Commented [AES11]: Enumerar todos los riesgos no

Commented [AES12]: Si la evaluación de riesgos fue realizada

Commented [AES13]: Si la evaluación de riesgos se realizó de

Commented [AES14]: Por ej. gerente de continuidad de

Commented [AES15]: Por ej. gerente de continuidad de

Commented [AES16]: Las acciones preventivas y el Plan de

Commented [AES17]: Para obtener más información sobre las estructuras de gestión de incidentes, lea este artículo:

Commented [AES18]: Para obtener más información sobre este tema, lea este artículo:

Commented [AES19]: Adaptar al sistema de identificación

Commented [AES20]: Evaluar si estas son los mejores roles

Commented [AES21]: Generalmente es alguien con la

El Gabinete de apoyo de crisis tiene la función de relevar al Gabinete de crisis de tareas administrativas y de otras actividades operativas para que pueda concentrarse en solucionar el incidente disruptivo.

Commented [AES22]: Adaptar al sistema de identificación estándar de la organización.

Los miembros del Gabinete de apoyo de crisis son:

- [secretarios/as]
- [mensajeros]
- [personal de seguridad]
- [personal para reparación de equipos no-crisis de TI]
- [otro personal de apoyo]

Commented [AES23]: Estos son solo ejemplos. Puede eliminar o agregar nuevos según la práctica de su organización.

El Gabinete de apoyo de crisis trabajará en ubicaciones especificadas por el Gabinete de crisis.

4.1.3. Equipamiento del Centro de crisis

Para que puedan funcionar el Gabinete de crisis y el Gabinete de apoyo de crisis, el Centro de crisis debe estar equipado de la siguiente manera:

[Nombre del recurso]	[Descripción]	[Cantidad]	[Cuando es necesario el recurso]
Aplicaciones / bases de datos:			
Datos almacenados en formato electrónico:			
[Estrategia de continuidad de negocio y plans para todas las actividades]			[Dentro de las 2 horas]
Datos almacenados en papel:			
[Estrategia de continuidad de negocio y plans para todas las actividades]			[Inmediatamente]
Equipos de TI y comunicaciones:			
[Impresoras de trabajo]			[Dentro de las 2 horas]
[Teléfonos]			[Inmediatamente]
[Teléfonos móviles]			[Inmediatamente]
[Impresoras]			[Dentro de las 2 horas]
[Equipo de TI]			[Inmediatamente]
Canales de			

Commented [AES24]: Según la cantidad de miembros del Gabinete de crisis y, en caso de ser necesario, del Gabinete de apoyo de crisis.

comunicación:			
[illegible]			[illegible]
[illegible]			[illegible]
Otros equipos:			
[illegible]			[illegible]
[illegible]			[illegible]
Instalaciones e infraestructura:			
[illegible]			[illegible]
[illegible]			[illegible]
Servicios externos:			
[illegible]			[illegible]

El [cargo] es el responsable de la preparación del Gabinete de crisis y del Gabinete de apoyo de crisis para que conozcan su función durante un incidente disruptivo. [illegible]

Commented [AES25]: Por ej. gerente de continuidad del [illegible]

Commented [AES26]: Por lo general, se trata de alguien con [illegible]

4.2. Comunicación y toma de decisiones

Los incidentes son comunicados de la siguiente forma:

- [illegible]
- [illegible]

Commented [AES27]: Este es un ejemplo de un proceso de [illegible]

Commented [AES28]: Ej. jefe del departamento de TI

Commented [AES29]: Ej. oficial de seguridad

Si las personas mencionadas no pueden resolver el incidente, deben informar al gerente de crisis, que decidirá si es necesario activar los planes de recuperación.

Las autorizaciones para la toma de decisiones son las siguientes:

[illegible]	[illegible]
Cómo se solucionan incidentes menores relacionados con tecnología de información y comunicación.	Empleados en [nombre de la unidad organizativa].
Cómo se solucionan otros incidentes menores.	Empleados en [nombre de la unidad organizativa].
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Commented [AES30]: Por lo general, se trata de alguien con [illegible]

Commented [AES31]: Ej.: gerente de compras.

Commented [AES32]: Ej.: analista de compras.

[redacted]	

El [cargo] es el responsable de preparar a los empleados de [nombre de la unidad organizativa] para que reconozcan y reaccionen ante incidentes relacionados con tecnología de la información y comunicación. [redacted]

Commented [AES33]: Ej.: jefe del departamento de TI.

Commented [AES34]: Ej.: gerente de continuidad de negocio.

4.3. Colaboración con las autoridades

Las siguientes personas están a cargo de la colaboración con las autoridades públicas y con los servicios de emergencia:

[redacted]	[redacted]
Policía	[cargo]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Commented [AES35]: Enumerar todas las demás autoridades [redacted]

Las personas mencionadas deben implementar todas las actividades preliminares para garantizar que la inter-operatividad con las autoridades durante el incidente disruptivo sea de un nivel satisfactorio. [redacted]

4.4. Evacuación del edificio y puntos de encuentro

Cada edificio es evacuado de acuerdo a lo especificado en el plan de evacuación de edificios en caso de incendios.

Commented [AES36]: Si no existe ese plan, es necesario [redacted]

Luego de evacuar el edificio, los empleados deben reunirse en los siguientes puntos de encuentro:

	Punto de encuentro 1	[redacted]
[redacted]		
[redacted]		
[redacted]		
[redacted]		

Commented [AES37]: Estas son, generalmente, lugares [redacted]

Nota: Si no está disponible el Punto de encuentro 1, los empleados deben reunirse en el Punto de encuentro 2.

[redacted]

Commented [AES38]: Por. ej. gerente de continuidad del [redacted]

4.5. Medios de comunicación

Commented [AES39]: Para obtener más información sobre este tema, lea este artículo: [redacted]

En caso de un incidente disruptivo, se utilizarán los siguientes medios de comunicación (las que se encuentran al principio de la lista se utilizarán primero, las que están cerca del final, se usarán sólo si las primeras no están disponibles):

1. teléfonos móviles (corporativos y privados)
2. teléfonos (corporativos y privados)
3. correo electrónico (enviado desde ordenadores corporativos o privados)
4. [correos de mensajería, por ej., Skype]
5. mensajeros (empleados de la organización o servicios especializados)
6. [señales de humo; establecer dónde serán guardadas y quién puede utilizarlas]
7. [señales de radioaficionado; establecer dónde serán guardadas y quién puede utilizarlas]
8. [teléfonos satelitales; establecer dónde serán guardados y quién puede utilizarlos]

El [cargo] es el responsable de adquirir, preparar y, cuando sea necesario, mantener, los medios de comunicación mencionadas para garantizar su disponibilidad durante un incidente disruptivo.

Commented [AES40]: Estos son solo ejemplos. Puede eliminar

Commented [AES41]: P.ej. gerente de continuidad del negocio,

4.6. Transporte hacia las ubicaciones alternativas

Los empleados de la organización serán trasladados desde la ubicación primaria hacia la alternativa de las siguientes formas:

[Actividad]	[Medio de transporte]
Gabinete de crisis y Gabinete de apoyo de crisis	[a pie, en auto privado, en auto corporativo, en autobús alquilado, en transporte público]
[actividad]	

Commented [AES42]: Se debe escoger un medio de transporte

Commented [AES43]: Enumerar todas las actividades.

El [cargo] es el responsable de proporcionar todos los medios de transporte.

Commented [AES44]: Por ej.: gerente de instalaciones.

4.7. Comunicación con las partes interesadas

[Nombre de la organización] manejará las relaciones con las diversas partes interesadas a través de la designación de personas que, ante un incidente disruptivo, se comunicarán con ellos a través de los siguientes medios de comunicación:

Commented [AES45]: Incluya el nombre de su organización.

	[Teléfono]	[Mensajero]	[Correo electrónico]	[Teléfono de emergencia]	[Medios públicos]		
[Empleados]							
[Propietarios / accionistas]							
[Proveedores de suministros]							
[Vecinos]							
[Medios públicos]							
[Reguladores]							
[Servicios de emergencia]							
[Otras partes interesadas]							

Commented [AES46]: Para cada medio de comunicación

El [cargo] es el responsable de preparar a todas las personas mencionadas anteriormente para realizar las comunicaciones en casos de incidentes disruptivos.

Commented [AES47]: Ej.: gerente de continuidad de negocio.

[redacted]

Commented [AES48]: Ej. gerente de continuidad de negocio, [redacted]

5. Estrategia para los recursos

5.1. Soluciones para ubicaciones e infraestructura

Las ubicaciones de recuperación de [nombre de la organización] son las siguientes:

Commented [AES49]: Incluya el nombre de su organización.

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Centro de crisis	[domicilio]	[a) ubicaciones alternativas dentro de la organización (por ej., si la misma organización tiene otras ubicaciones a su disposición); [redacted]]		[a) frío, b) templado, [redacted]]	[domicilio]	[domicilio]

Commented [AES51]: Esta ubicación, generalmente se [redacted]

Commented [AES52]: Esta ubicación, generalmente se encuentra, como mínimo, a 40 km de la ubicación principal.

[redacted]

Commented [AES50]: Según la cantidad de personas en una [redacted]

[nombre de la actividad]	[domicilio]				[domicilio]	[domicilio]

Commented [AES53]: Seleccione al menos una de las

Commented [AES54]: Enumere todas las actividades críticas,

*Los términos utilizados en esta columna tienen el siguiente significado:

a) Frío: ubicación sin infraestructura ni equipos.

c) Caliente: ubicación que cuenta infraestructura preinstalada, con todos los equipos, enlaces y software.
d) Equipo: ubicación con la infraestructura, todo los equipos, enlaces y software instalados previamente y con datos en tiempo real.

El [cargo] es el responsable de realizar todos los preparativos necesarios relacionados con las ubicaciones alternativas. El [cargo] es el responsable de equipar a las ubicaciones alternativas.

Commented [AES55]: Ej.: gerente de instalaciones.

Commented [AES56]: Ej. gerente de TI, gerente de

5.2. Soluciones para proveedores y socios

Las relaciones con los proveedores y socios deben ser manejadas de la siguiente forma:

[redacted]	[redacted]
	[a] Se contratan servicios a diversos proveedores o socios en forma simultánea; si alguno de ellos no está disponible, se pueden utilizar los servicios de otro). b) Estimular u obligar a los proveedores o socios a aumentar el nivel de su capacidad para la continuidad de negocio (de esta manera se reduce el riesgo de ocurrencia de un incidente y de sus consecuencias). c) Obligar por contrato a los proveedores o socios a la entrega de mercancías o servicios independientemente del incidente disruptivo y definir sanciones (de esta manera, los proveedores o socios están obligados implementar la continuidad de negocio y, a la vez, se traslada o elimina una parte del riesgo financiero). d) Determinar proveedores o socios alternativos (de esta forma, se puede preparar el traslado de actividades de negocio, aunque la relación comercial no se mencionará que se produzca un incidente disruptivo). e) Preparar de las actividades a la organización (se prepara a la organización para reforzar las actividades que hayan sido externalizadas.)

Commented [AES57]: Informar los nombres de todos los

Commented [AES58]: Seleccionar una o más de las opciones

El [cargo] es responsable de gestionar las relaciones con los proveedores y con los socios externos para garantizar que la inter-operabilidad durante un incidente disruptivo sea de un nivel satisfactorio.

Commented [AES59]: Ej.: gerente de compras, gerente de

5.3. Soluciones para aplicaciones / bases de datos

Todas las aplicaciones y bases de datos necesarias estarán instaladas en la ubicación alternativa dentro de las 24 horas de producido el incidente disruptivo; para aquellas aplicaciones y bases de

datos que no son necesarias dentro de las 24 horas, los medios de instalación se almacenarán en la ubicación alternativa.

[Cargo] es el responsable de la instalación de aplicaciones y bases de datos y de la preparación de los medios de instalación.

Commented [AES60]: Ej.: gerente de TI

5.4. Datos

Se deben realizar copias de seguridad de los datos compartidos por varias actividades con los siguientes intervalos:

[Nombre de la aplicación, base de datos, carpeta, documento]	[Frecuencia para creación de copias de seguridad]	[Procedimiento para copias de seguridad]
		[(a) aplicaciones / bases de datos: procedimiento de respaldo automatizado basado en servidor; b) documentos electrónicos: almacenamiento en carpetas de Intranet para las cuales se crean copias de seguridad en forma automática; c) documentos en papel: recepción de todos los documentos de fax por medios electrónicos, y escaneo y copia de los documentos y almacenamiento en dos lugares separados.]

Commented [AES61]: Copiar del Cuestionario sobre el análisis [...]

Commented [AES62]: La frecuencia se determina en base a los [...]

Commented [AES63]: Según el tipo de datos, seleccionar la [...]

Nota: la frecuencia para crear copias de seguridad de los datos utilizados por una única actividad se define en la estrategia para dicha actividad.

[Cargo] es el responsable de la creación de copias de seguridad para los datos mencionados anteriormente.

Commented [AES64]: Si hay varios grupos de datos, se puede [...]

5.5. Evitar un punto único de falla

Se utilizan las siguientes estrategias para evitar un punto único de falla, que puede ocasionar la interrupción de una actividad:

Punto único de falla	[illegible]	[illegible]

Commented [AES65]: Copiar del Cuestionario sobre el análisis [illegible]

Commented [AES66]: Plan para recursos alternativos o de [illegible]

El [cargo] es el responsable de implementar la estrategia para evitar la ocurrencia de un punto único de falla.

Commented [AES67]: Si hay varios tipos de puntos únicos de [illegible]

5.6. Suministro de recursos financieros

[Nombre de la organización] necesita [cantidad en moneda local] para capital de trabajo para todas las actividades, más [monto en moneda local] para compras de emergencia en caso que se produzca un incidente disruptivo.

Commented [AES68]: Incluya el nombre de su organización.

Commented [AES69]: Calcular de los cuestionarios sobre el [illegible]

Commented [AES70]: Calcular el costo de todos los recursos [illegible]

En caso de producirse un incidente disruptivo, los recursos financieros serán suministrados de la siguiente forma: (a) una organización mantendrá en forma constante el nivel necesario de liquidez en dinero en [illegible]; (b) se suscribirá un contrato de financiación contingente con [nombre de la institución financiera]; (c) [nombre de la persona] otorgará un préstamo privado o (d) [nombre de los proveedores y socios externos] ampliarán las condiciones de pago.

Commented [AES71]: Especificar otros instrumentos [illegible]

El [cargo] es el responsable de realizar todos los preparativos necesarios relacionados con la provisión de recursos financieros.

Commented [AES72]: Por lo general, se trata de alguien con [illegible]

6. Estrategia de recuperación para actividades individuales

La estrategia de recuperación para actividades individuales y soluciones para implementar esas estrategias se definen en los Apéndices 4 a [número] de la presente Estrategia.

La persona designada como gerente de recuperación para una actividad individual es la responsable de la redacción de los Planes de recuperación para dicha actividad. El [cargo] es el responsable de preparar todos los recursos necesarios para actividades individuales.

Commented [AES73]: Por lo general, se trata de alguien con [illegible]

7. Implementación de todos los preparativos necesarios

El Apéndice 3 enumera todos los preparativos necesarios para la implementación de esta Estrategia y soluciones relacionadas. El [cargo] debe definir los recursos financieros y de otra naturaleza necesarios y debe definir plazos para la implementación de cada preparativo; y el [cargo] está a cargo de supervisar la coordinación y ejecución de todas las acciones preparativas, como también de informar sobre su implementación.

Commented [AES74]: Por lo general, se trata de alguien con [illegible]

Commented [AES75]: Ej. gerente de continuidad de negocio, [illegible]

8. Gestión de registros guardados en base a este documento

Nombre del registro	*Ubicación de archivo*	[illegible]	[illegible]	[illegible]
Plan de preparación para continuidad de negocio (en formato electrónico).	Ordenador de [cargo responsable de supervisar la ejecución].	[illegible]	[illegible]	[illegible]

Commented [AES76]: Inserte los datos en esta columna para [illegible]

Commented [AES77]: Ej. gerente de continuidad de negocio, [illegible]

9. Validez y gestión de documentos

Este documento es válido hasta el [fecha].

[illegible] **Commented [AES78]:** Ej. gerente de continuidad de negocio, [illegible]

Commented [AES79]: Esto es sólo una recomendación; ajustar [illegible]

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Si la organización tuvo éxito en la recuperación de las actividades críticas dentro del objetivo de tiempo de recuperación.
- [illegible]

10. Apéndices

- Apéndice 1: Objetivos de tiempo de recuperación para actividades
- Apéndice 2: Ejemplos de escenarios de incidentes disruptivos
- [illegible]

Commented [AES80]: Ingresar para cada actividad crítica, [illegible]

[cargo]
[nombre]

[firma]

Commented [AES81]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.