

[línea horizontal]

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 the Business Impact Analysis Methodology 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]

METODOLOGÍA PARA EL ANÁLISIS DE IMPACTO EN EL NEGOCIO

Commented [AES3]: Para conocer acerca del análisis de impactos en el negocio, lea el siguiente artículo:

How to implement business impact analysis (BIA) according to ISO 22301 <https://advisera.com/27001academy/knowledgebase/how-to-implement-business-impact-analysis-bia-according-to-iso-22301/>

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.....3
- 2. DOCUMENTOS DE REFERENCIA.....3
- 3. METODOLOGÍA PARA EL ANÁLISIS DEL IMPACTO EN EL NEGOCIO3
 - 3.1. ORGANIZACIÓN 3
 - 3.2. IDENTIFICACIÓN DE ACTIVIDADES..... 3
 - 3.3. IMPACTOS DEL INCIDENTE DISRUPTIVO..... 3
 - 3.4. DETERMINACIÓN DE LA INTERRUPCIÓN MÁXIMA ACEPTABLE 4
 - 3.5. CANTIDAD DE TRABAJO..... 4
 - 3.6. RECURSOS NECESARIOS PARA LA RECUPERACIÓN 5
 - 3.7. DEPENDENCIA DE TERCEROS 5
 - 3.8. PÉRDIDA MÁXIMA DE DATOS..... 5
 - 3.9. PRESENTACIÓN DE LOS RESULTADOS 6
 - 3.10. REVISIÓN PERIÓDICA DEL ANÁLISIS DEL IMPACTO EN EL NEGOCIO 6
- 4. GESTIÓN DE REGISTROS GUARDADOS EN BASE A ESTE DOCUMENTO6
- 5. VALIDEZ Y GESTIÓN DE DOCUMENTOS7
- 6. APÉNDICES7

1. Objetivo, alcance y usuarios

El objetivo de este documento es definir la metodología y el proceso para evaluar los impactos de la interrupción de las actividades de [nombre de la organización] y determinar prioridades y objetivos de continuidad y de recuperación.

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

El análisis del impacto en el negocio se aplica a todo el alcance del Sistema de Gestión de Continuidad de Negocio (SGCN); es decir, a todas las actividades que sustentan los productos y servicios de [nombre de la organización].

Commented [AES6]: Si solo se implementa la seguridad de la información (no continuidad de negocio), reemplazar por este texto: "Sistema de Gestión de Seguridad de la Información (SGSI)".

Los usuarios de este documento son todos los empleados de [nombre de la organización] que participan en el establecimiento e implementación del SGCN.

Commented [AES7]: Incluya el nombre de su organización.

Commented [AES8]: Incluya el nombre de su organización.

Commented [AES9]: O 'SGSI'

2. Documentos de referencia

- Norma ISO 22301 cláusulas 8.2.1 y 8.2.2
- Norma ISO 27001 cláusula A.5.29
- Política de continuidad de negocio
- Estrategia de continuidad de negocio
- Lista de requisitos legales, normativos, contractuales y de otra índole

Commented [AES10]: Puede encontrar una plantilla para este documento en la carpeta del Paquete Premium de documentos sobre ISO 27001 e ISO 22301 "03_Identificación_de_requisitos".

3. Metodología para el análisis del impacto en el negocio

Commented [AES11]: Se debe modificar esta Metodología si...

3.1. Organización

El análisis del impacto en el negocio se implementa a través de los Cuestionarios sobre el análisis del impacto en el negocio. El proceso es coordinado por [cargo] y el análisis de las actividades individuales es realizado por la persona responsable de cada actividad.

Commented [AES12]: Para obtener más información sobre este tema, lea este artículo:

El análisis del impacto en el negocio se realiza con los Cuestionarios de análisis de impacto en el negocio para cada actividad. El proceso es coordinado por [cargo] y el análisis de las actividades individuales es realizado por la persona responsable de cada actividad.

Commented [AES13]: Por ejemplo, gerente de continuidad de...

El proceso de documentos de referencia utilizados de acuerdo a esta Metodología se detallan en [lista de documentos].

Commented [AES14]: Por ej., Política de clasificación de la...

3.2. Identificación de actividades

El [cargo] es responsable de identificar todas las actividades que sustentan la provisión de productos y servicios y de designar la persona responsable para cada actividad.

Commented [AES15]: Por ejemplo, gerente de continuidad de...

3.3. Impactos del incidente disruptivo

Los impactos de un incidente disruptivo sobre una actividad son evaluados a través de los (1) impactos generales (evaluación cualitativa) e (2) impacto financiero (evaluación cuantitativa). Ambos impactos son evaluados para los siguientes periodos de tiempo:

- 2 horas
- 4 horas
- 8 horas
- 1 semana

Si alguna actividad es menos urgente, se pueden alargar los periodos para esa actividad particular; por ej., de 4 horas a 2 semanas, o similar.

Para la evaluación general (1), los impactos se clasifican de la siguiente forma:

Consecuencia insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia menor	2	La duración del incidente disruptivo afecta levemente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero no de forma suficiente para ser aceptable cuando se evalúa la integridad o continuidad operativa.
Consecuencia moderada	3	La duración del incidente disruptivo afecta moderadamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y no de forma suficiente para ser aceptable por su integridad o continuidad operativa.
Consecuencia severa	4	La duración del incidente disruptivo afecta gravemente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y no de forma suficiente para ser aceptable por su integridad o continuidad operativa.

Para la evaluación financiera (2), el impacto tiene que ser establecido en moneda local.

3.4. Determinación de la Interrupción máxima aceptable

La Interrupción máxima aceptable (MAO, por sus siglas en inglés) o Período máximo tolerable de interrupción se determina en horas o días, de la siguiente forma:

- El tiempo más corto antes del cual el impacto general es nivel 3 (o nivel 4 si no está definido el 3), o
- El tiempo más corto antes del cual el impacto financiero es aceptable en comparación con la actividad que se está evaluando.

3.5. Cantidad de trabajo

En esta parte del análisis se identifican los periodos con los picos de mayor carga de trabajo y se establecen los objetivos mínimos de continuidad de negocio.

3.6. Recursos necesarios para la recuperación

Es necesario identificar los siguientes tipos de recursos:

- Personas
- Aplicaciones / bases de datos
- Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos)
- Datos almacenados en papel
- Copias de Tercer conmutación
- Copias de comunicación
- Otros recursos
- Logística y transporte
- Instalaciones o infraestructuras
- Capital de trabajo
- Servicios externos

Para cada recurso es necesario determinar las siguientes necesidades:

- Cantidad de recursos que se requieren para la recuperación de una actividad
- Si el recurso es crítico o no (Puede ser de alta)
- Tiempo que puede transcurrir desde que se necesita el recurso (tiempo permitido a la recuperación de la actividad)

3.7. Dependencia de terceros

En esta parte del análisis es necesario identificar la dependencia en relación a (1) otras actividades, (2) socios externos y (3) proveedores.

Para cada socio externo y proveedor es necesario analizar lo siguiente:

- Qué documentos define las relaciones en caso de un incidente de seguridad
- El nivel máximo de capacidad para la continuidad de negocio

3.8. Pérdida máxima de datos

Para cada base de datos, aplicación o pieza de información identificada en el análisis, es necesario evaluar la cantidad máxima de datos que se pueden perder. La pérdida de datos se evalúa por la cantidad de datos creada en las últimas:

- 1 hora
- 4 horas
- 24 horas
- 48 horas
- 72 horas

Si es necesario, se puede evaluar o elegir la cantidad de una actividad particular para que se quede el tipo de datos de dicha actividad.

El impacto de la pérdida de datos se clasifica de la siguiente forma:

Consecuencia insignificante	1	La cantidad de datos perdidos no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia menor	2	La cantidad de datos perdidos podría afectar las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero no de una manera que sea probable o inevitable en cuanto a magnitud o consecuencias específicas.
Consecuencia mayor	3	La cantidad de datos perdidos podría afectar las finanzas, las obligaciones legales o contractuales o el prestigio de la organización de una manera que sea probable o inevitable en cuanto a magnitud o consecuencias específicas.
Consecuencia crítica	4	La cantidad de datos perdidos podría afectar las finanzas, las obligaciones legales o contractuales o el prestigio de la organización de una manera que sea probable o inevitable en cuanto a magnitud o consecuencias específicas.

3.9. Presentación de los resultados

La información recabada mediante los Cuestionarios sobre el análisis del impacto en el negocio se envía a [cargo], que tiene la responsabilidad de reunir y documentar los datos a través de la Estrategia de continuidad de negocio.

Commented [AES16]: Por ejemplo, gerente de continuidad de negocio.

3.10. Revisión periódica del análisis del impacto en el negocio

El [cargo] debe realizar una revisión de los Cuestionarios sobre el análisis del impacto en el negocio y, en función de ello, debe actualizar la Estrategia de continuidad de negocio.

Commented [AES17]: Por ejemplo, gerente de continuidad de negocio.

4. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Forma de guarda de los registros	Período de retención
Cuestionarios sobre el análisis del impacto en el negocio (formulario electrónico, documento de Excel)	Ordenador del [cargo]	[cargo]	Los cuestionarios deben ser guardados en formato de archivo único.	Se debe conservar por un período de 7 años.

Commented [AES18]: Adapte el período en esta columna a sus necesidades.

Commented [AES19]: Por ejemplo, gerente de continuidad de negocio.

Solamente el [cargo] puede permitir a otros empleados el acceso a los documentos mencionados precedentemente.

5. Validez y gestión de documentos

Este documento es válido desde el [fecha].

El responsable de este documento es el [cargo], con título [cargo] y, a su vez, actualiza el documento por lo menos [frecuencia] antes de la revisión periódica sobre los Cuestionarios sobre el análisis del impacto en el negocio.

Commented [AES20]: Por ejemplo, gerente de continuidad de negocio, gerente de riesgos, etc.

Commented [AES21]: Esto es sólo una recomendación; ajustar [frecuencia] según sea necesario.

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

- La cantidad de recursos no incluidos en los Cuestionarios sobre el análisis de la continuidad de negocio.
- La oportunidad de recuperar actividades críticas o esenciales en el proceso de análisis del impacto en el negocio.
- La cantidad de errores en el proceso de análisis del impacto en el negocio debido a deficiencias para falta de roles y responsabilidades.

6. Apéndices

- Apéndice 1 – Cuestionario sobre el análisis de impacto en el negocio

[cargo]

[nombre]

[firma]

Commented [AES22]: Sólo es necesario si el Procedimiento para el control de documentos y registros establece que los documentos en papel deben ser firmados.