



M-SGI-008 Metodología BIA

Responsables

Elaboró:	Líder del SGI
Revisó:	Gerente de normatividad y cumplimiento
Aprobó:	Dirección General

Control de versiones

Versión	Fecha	Descripción del cambio
1	15/08/2022	Emisión inicial

Contenido

1. Introducción.....	3
2. Alcance	3
3. Definiciones.....	3
4. Descripción del manual.....	5
5. Anexos.....	20

1. Introducción

El análisis que permita calificar y cuantificar el impacto derivado de una interrupción en las operaciones, así como, de las infraestructuras consideradas como críticas, es importante a considerarse antes de cualquier definición de estrategia de continuidad. Con base en dicho análisis es posible determinar las necesidades y recursos humanos, materiales y de procesamiento en una situación de contingencia, así como evaluar las opciones de respaldo y recuperación que mejor se ajusten a las necesidades expuestas.

El Análisis de impacto al Negocio (BIA) según las mejores prácticas, “Es el proceso de analizar las actividades y el efecto que una interrupción del negocio puede tener sobre éstas” y en la medida en que se identifiquen y comprendan los impactos, se podrán desarrollar estrategias, planes de continuidad de las operaciones y planes de recuperación ante desastres efectivos que minimicen las afectaciones identificadas en caso de una interrupción. Este proceso de análisis deberá llevarse a cabo al menos una vez al año cuando existan cambios significativos en la organización.

2. Alcance

El análisis de impacto al negocio y de impacto a los aplicativos es de aplicación general, contemplando al personal, los procedimientos, la infraestructura, sistemas tecnológicos, información y a los proveedores internos o externos que participen de forma habitual o esporádica en la ejecución de los procesos, definidos para los procesos del alcance del Sistema de Gestión de Continuidad de Negocio.

3. Definiciones

Análisis de Impacto al Negocio (BIA, por sus siglas en inglés): También se le puede identificar como Análisis de Impacto a las Operaciones (AIO, por sus siglas en inglés) y es el estudio de funciones de una organización y los efectos que una interrupción podría tener sobre ellos, este análisis permite identificar y priorizar los procesos críticos.

Análisis de Riesgos (RA, por sus siglas en inglés): Es un trabajo de investigación e interpretación de las amenazas que podrían causar un evento disruptivo a una organización, su identificación permite sugerir un tratamiento para minimizar la probabilidad de ocurrencia. Tanto el Informe de Riesgos, como la Metodología para el Análisis de Riesgos son documentos independientes al presente, sin embargo, se encuentran relacionados al proceso de Continuidad de Negocio.

Clasificación de respaldos: Los respaldos se pueden catalogar en respaldos físicos, electrónicos o en incluso híbridos, es decir, en ambos formatos.

Contingencia: Evento no planeado que inhabilita a una organización, o a una parte de ella, para operar sus procesos por un período de tiempo tal que pueda ocasionar un daño o pérdida a un nivel inaceptable.

Continuidad del Negocio (BC, por sus siglas en inglés): Capacidad de una organización para continuar con la entrega de sus servicios críticos a niveles predefinidos aceptables, después de un incidente de interrupción.

Disponibilidad Tecnológica: es la garantía que se le proporciona al usuario para el acceso en el tiempo y forma que necesiten a los sistemas, redes e información que previamente se les haya designado. Como tal, la Disponibilidad Tecnológica se identifica posterior al Análisis de Impacto al Negocio y se encuentra asociada Plan de Recuperación de Desastres que es un documento independiente a este.

Estrategia de Recuperación y Continuidad: es el plan predefinido para reestablecer las operaciones de los procesos que hayan sufrido alguna interrupción, mismo que se debe encontrar dentro del Plan de Continuidad de Negocio cuyo documento se obtiene posterior al Análisis de Impacto al Negocio.

Máximo Tiempo de Interrupción Tolerable (Maximun Tolerable Period of Disruption): Es la suma de RTO y WRT, y se define como el periodo de tiempo de inactividad máximo tolerable en total que puede interrumpirse un proceso sin causar consecuencias aceptables.

Monitoreo y Actualización: son las actividades alineadas a las buenas prácticas internacionales de Continuidad de Negocio y que le permiten a la empresa conservar, renovar, mejorar y si fuera el caso modificar las estrategias.

Periodo más crítico del proceso: Tomando como referencia este momento, se puede apoyar a determinar el RTO, basándose en la idea de realizar el análisis considerando el peor escenario posible.

Plan de continuidad: indica los insumos técnicos, humanos, roles específicos y organización interna que garanticen la continuidad de las operaciones tecnológicas.

Plan de Continuidad del Negocio (BCP, por sus siglas en inglés): Conjunto de procedimientos documentados que guían a las organizaciones a responder, recuperar, reanudar y restaurar la operación de los procesos y los servicios a un nivel predefinido posterior a una interrupción. Por lo general incluye los recursos, servicios y actividades necesarias para garantizar la continuidad de las funciones críticas.

Procesos Críticos: Son aquellos procesos que, en caso de sufrir una interrupción, tienen el mayor impacto en la generación y entrega de los servicios de la organización. Este impacto se manifiesta en un muy corto plazo después de una interrupción.

Pruebas y Simulacros: son los ejercicios documentados para identificar áreas de oportunidad y mejora del Plan de Continuidad de Negocio, los procedimientos se describirán dentro del Plan de Pruebas y Simulacros.

Punto objetivo de recuperación (RPO, por sus siglas en inglés): Se asocia a la cantidad de información que puede perderse en un proceso en caso de interrupción sin que esta pérdida genere un impacto grave para la organización. Esta medida se expresa en unidades de tiempo.

Recursos en Contingencia: Indica el nivel mínimo aceptable de recursos humanos (personal crítico), tecnológicos y materiales del proceso durante una indisponibilidad. Indica si el proceso puede operarse parcialmente obviando algunos recursos o con una eficiencia menor sin que exista una afectación mayor para la organización. Es decir, al estar en contingencia, no se recuperan los procesos completamente, sino lo mínimo indispensable para no elevar los impactos.

Registros Vitales: Se refiere a toda aquella documentación necesaria para la ejecución del proceso y es importante identificar la ubicación del respaldo de la información o en su defecto, su carencia.

Retorno a la Normalidad: o también conocido como Vuelta a Casa, está contenido en el Plan de Restauración y Reinicio de actividades, el cual incluirá las instrucciones que serán entregadas al responsable del Plan de Continuidad de Negocio para indicarle al personal crítico el término de la contingencia.

Riesgo: La probabilidad de que una amenaza pueda explotar una vulnerabilidad, generando un impacto sobre la infraestructura de TIC y los activos de información sobre la empresa

Servicios Core: Son aquellas actividades principales o de gran valor para toda la organización.

Tiempo de Trabajo en Recuperación (Work Recovery Time): Es la cantidad de tiempo en el que los procesos son ejecutados durante la recuperación con los recursos mínimos necesarios y determina la cantidad máxima de tiempo requerido para verificar la integridad de los sistemas y de los datos.

Tiempo objetivo de recuperación (RTO, por sus siglas en inglés): Es el tiempo en el que los procesos deberían ser recuperados antes de generar un impacto grave o catastrófico para la organización.

4. Descripción del manual

Para la ejecución del Análisis de Impacto al Negocio es importante comprender las necesidades y requerimientos de la empresa en materia de continuidad de negocio, tanto con los usuarios internos, como con sus usuarios externos, así como, con las partes interesadas en materia legal o normativa, esto con la finalidad de determinar el alcance y procesos críticos. Considerando los requerimientos legales, normativos, contractuales, de infraestructura y de personal requerido para brindar los servicios del alcance del SGCN, se define el siguiente modelo para su elaboración:

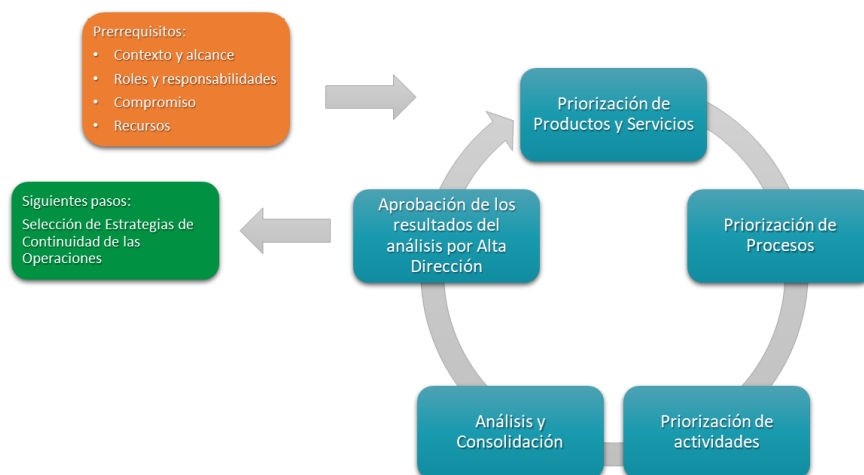


Figura. 1 Modelo Análisis de Impacto al Negocio



Para llevar a cabo el BIA, **SILENT4BUSINESS**, Definirá el objetivo y alcance de la Gestión de Continuidad del Negocio, estrategias, procedimientos y acciones que permiten, ante la verificación de Contingencias Operativas, la continuidad en la prestación de los servicios o en la ejecución de los procesos críticos de la empresa, o bien su restablecimiento oportuno, así como la mitigación de las afectaciones producto de dichas contingencias, para esto, desarrollará las siguientes actividades y documentos:

a) **Prerrequisitos:** Identificación y entendimiento de la estructura de continuidad de negocio de la empresa, la cual deberá consolidarse con los requisitos identificados en el Contexto de la organización bajo los cuales la empresa desempeña las diversas actividades Core de sus servicios. Para esto **SILENT4BUSINESS** contemplará lo siguiente:

- Descripción de los productos y/o servicios, procesos, sus asociaciones
- Cadenas de abastecimiento (información)
- Relación entre la política de continuidad de negocio con los objetivos institucionales y la estrategia de gestión de riesgos
- Apetito de riesgo
- Roles y responsabilidades en materia de continuidad de negocio

Una vez identificados los prerequisites, así como, el contexto de la empresa, **SILENT4BUSINESS** conforme a los requerimientos de la metodología de Análisis de Impacto al Negocio (BIA) basada en las mejores prácticas, llevará a cabo la priorización de información en 3 niveles, esto con la finalidad de obtener y explotar la información en un carácter descendente, el cual, permita emitir recomendaciones alineadas a las necesidades reales de la empresa, siendo estos:



Figura. 2 Niveles de priorización.

- Priorización de los productos y/o servicios:** Conforme al análisis de contexto de la organización, así como, de las necesidades y requerimientos de las partes interesadas y los prerequisites, se llevará a cabo la priorización de los productos y/o servicios de la empresa, identificando aquellos productos y/o servicios indispensables que ante un evento de contingencia deben continuar su operación bajo el porcentaje mínimo aceptable definido por la empresa en un ambiente de contingencia.
- Priorización de procesos:** Una vez priorizados los productos y/o servicios considerados como indispensables para la empresa, se llevará a cabo la identificación de los procesos críticos que soportan la ejecución de los productos y/o servicios analizados y que en caso de una contingencia deberán ser considerados dentro de las estrategias de recuperación y los planes de continuidad.
- Priorización de actividades:** Con las priorizaciones anteriores y contando con toda la información requerida de los niveles estratégicos y tácticos, se llevará a cabo la identificación de actividades con las que se ejecutan o se vuelven factores críticos en la consecución de los objetivos establecidos en los productos o servicios Core de la empresa.

Para llevar a cabo el levantamiento de información **SILENT4BUSINESS** conforme a las técnicas existentes en el mercado empleará para este ejercicio las siguientes estrategias en sus diversas etapas de ejecución:

- **Entrevistas:** Sesiones de trabajo previamente acordadas con los dueños o ejecutores de actividades que soportan los productos/servicios Core de la empresa.
- **Cuestionarios:** Con la finalidad de robustecer la información recabada en las entrevistas, se elaborarán cuestionarios con los elementos requeridos para la obtención de información del BIA y AR, la cual servirá de sustento para los dueños de los productos/servicios definidos como prioritarios o Core de la empresa.

La información relevante que coadyuva a generar una estrategia y que contendrán los cuestionarios para la ejecución de los diferentes Análisis por cada uno de los niveles es la siguiente:

- Información general de: productos, servicios, procesos y subprocesos/actividades.
- Número de transacciones o solicitudes.
- Periodo crítico en función de: meses, semanas, días y horas.
- Impactos en función de los periodos críticos.
- Tiempos de recuperación: RTO y RPO.
- Personal que se requiere para operar: Titular, Suplente y Supervisor (Normal / Critico).
- Entradas y salidas de procesos.
- Aplicaciones críticas.
- Registros vitales.
- Requerimientos (dispositivos) mínimos para la operación (Normal / Critico).
- Requerimientos especiales, sólo si aplicaran.
- Proveedores nombre y personal de contacto

Con base en lo anterior, **SILENT4BUSINESS** empleara el siguiente modelo para el levantamiento, análisis y elaboración de reportes del BIA:



Figura. 3 Modelo de levantamiento y análisis de información.

- **Tiempos de Recuperación:**

Para realizar el levantamiento de información, se debe considerar los siguientes tiempos de recuperación, ya que estos serán, entre otra información el insumo esencial para la determinación de las estrategias de recuperación:

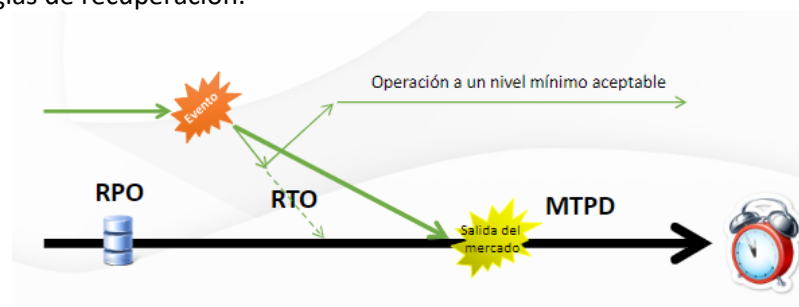


Figura. 1 Tiempos de Recuperación

RPO: Punto Objetivo de Recuperación (Recovery Point Objective), es la cantidad de información expresada en tiempo que podría perderse en caso de una interrupción del proceso sin que esta pérdida genere un impacto significativo.

RTO: Tiempo Objetivo de Recuperación (Recovery Time Objective), es el tiempo en el que los procesos deben ser recuperados antes de generar un impacto relevante a la empresa.

WRT: Tiempo de Trabajo en Recuperación (Work Recovery Time), es la cantidad de tiempo en el que los procesos son ejecutados durante la recuperación con los recursos mínimos necesarios y determina la cantidad máxima de tiempo requerido para verificar la integridad de los sistemas y de los datos.

MTPD: Máximo Tiempo de Interrupción Tolerable (Maximun Tolerable Period of Disruption), es la suma de RTO y WRT; y se define como el periodo de tiempo de inactividad máximo tolerable en total que puede interrumpirse un proceso sin causar consecuencias aceptables.

- **Escenarios de Contingencia**

Como parte de la metodología de Análisis de Impacto al Negocio, se establecen de manera enunciativa más no limitativa los escenarios de riesgo a los cuales la empresa puede estar expuesta, con base en la ubicación de las instalaciones, ubicación de centro de datos, lugar donde se resguarda la información de la empresa o clientes, el mercado en el que desarrolla sus actividades, número de personas, tipo de servicios entre otros; para ello se determinan los siguientes escenarios:

ESCENARIOS DE RIESGO
Desastres Naturales y Ambientales
Enfermedades Infecciosas
Ataques cibernéticos o a la actividad informática
Sabotaje
Terrorismo
Interrupción en el suministro de energía
Fallas o indisponibilidad en la infraestructura tecnológica (telecomunicaciones, procesamiento de información y redes)
Indisponibilidad de recursos humanos, materiales o técnicos
Interrupción en servicios prestados por terceros
Indisponibilidad de Instalaciones (oficinas), por bloqueo de acceso, manifestaciones.

Determinando su probabilidad de ocurrencia conforme a los siguientes criterios:

Nivel de Probabilidad	Criterios para la determinar la Probabilidad
5-Casi Cierto	Cuenta con antecedentes de ocurrencia frecuentes; es más probable que se presente a que no. Existen muchos factores y condiciones que propician su ocurrencia. (Cada semana) .
4-Muy probable	Cuenta con antecedentes de ocurrencia; es más probable que se presente a que no. Existen factores y condiciones que propician su ocurrencia. (Cada mes)
3-Probable	Cuenta con antecedentes, pero su ocurrencia ha sido ocasional; Es igual de probable se presente. Las condiciones son medianamente favorables para permitir su ocurrencia. (cada 3 meses) .
2-Poco Probable	No se tienen antecedentes de ocurrencia recientes o Cuenta con antecedentes, pero su ocurrencia ha sido ocasional; Es igual de probable se presente o no se presente. Las condiciones son mínimamente favorables para permitir su ocurrencia. (cada 6 meses) .
1-Remoto	No se tienen antecedentes de ocurrencia. Es probable que no se presente (no se cuenta con elementos para determinar si es más probable que suceda o que no suceda). Las condiciones son mínimamente favorables para permitir su ocurrencia. (cada año) .

Los que a su vez serán evaluados conforme a los siguientes criterios:

- **Criterios de Impacto**

Se propondrán con base en las mejores prácticas y estándares de continuidad de negocio el tipo de impacto que sea aplicable a la empresa, conociendo aquellos elementos que pudieran verse afectados en una contingencia y sus consecuencias sobre los procesos de negocio, para tal efecto los impactos sugeridos de manera enunciativa más no limitativa son:

TIPOS DE IMPACTO
Financiero
Operacional
Regulatorio o Normativo
Afectación en la Imagen, Reputacional
Medio ambiental
Social
Salud o Bienestar

- **Priorización de Tipos de Impacto**

Se realizará de manera numérica del 1 al N; dónde el numero 1 representa el impacto más crítico

para la empresa y el N representa el de menor criticidad.

TIPOS DE IMPACTO	ESCALA
Financiero	1
Operacional	2
Regulatorio o Normativo	3
Afectación en la Imagen, Reputacional	4
Ej. Medio ambiental	5
Ej. Social	6
Ej. Salud o Bienestar	7
Otro	N

**La asignación en la escala se puede ajustar conforme a los criterios y necesidades de la Silent4Business*

- Severidad del Impacto**

Se propondrá una definición del tipo de severidad de cada uno de los impactos aplicables a la empresa. Se puede medir con base en porcentajes de incumplimiento o pérdida, montos, sanciones y multas, población afectada, entre otros.

Se realizará de forma cuantitativa y cualitativa, indicando los niveles de afectación que se pudieran presentar en la empresa.

La siguiente tabla representa los tipos de impactos propuestos con sus respectivos niveles de severidad.

TIPOS DE IMPACTO	SEVERIDAD	DESCRIPCIÓN
Impacto Financiero	Critico	Pérdidas económicas mayores a ##### pesos
	ALTO	Pérdidas económicas entre ##### y ##### pesos
	MEDIO	Pérdidas económicas entre ##### y ##### pesos
	BAJO	Pérdidas económicas menores a ##### pesos
Afectación operacional	Critico	Suspende la operación o genera reprocesos mayores a 2 días.
	ALTO	Suspende la operación o genera reprocesos mayores a 1 día y hasta 2 días.
	MEDIO	Suspende la operación o genera reprocesos mayores a 4 horas y hasta 1 día.
	BAJO	Suspende la operación o genera reprocesos menores a 4 horas.
Impacto Regulatorio o Normativo	Critico	Podrían generarse penalizaciones, y/o investigación contra la empresa por faltas a normatividad Nacional o Constitucional.
	ALTO	Podrían generarse penalizaciones y/o investigación contra la empresa por faltas a los organismos reguladores (SAT, STPS, PROFECO, LFPDPPP, CONDUSEF, Etc.)

TIPOS DE IMPACTO	SEVERIDAD	DESCRIPCIÓN
Afectación en la Reputación / Imagen Pública o Política	MEDIO	Faltas a los procedimientos, políticas manuales y/o reglamentos organizacionales.
	BAJO	Sin afectación regulatoria o normativa.
	Critico	Cobertura mediática nacional y limitada a nivel internacional, pérdida seria de clientes, investigación formal del regulador, implicación de directivos.
	ALTO	Cobertura mediática a escala nacional, incremento en reclamaciones de clientes, pérdida de clientes, solicitud de información del regulador (informal).
	MEDIO	Cobertura mediática local o del sector, reclamaciones de clientes, posible pérdida de clientes.
	BAJO	Sin cobertura mediática o efecto externo.

- Evaluación de la Criticidad

El valor total del impacto estará dado en las siguientes categorías:

SEVERIDAD	VALOR
CRITICA	4
ALTO	3
MEDIO	2
BAJO	1

Para determinar los límites de los impactos, por cada tipo se le será asignado un número de acuerdo con la sucesión de Fibonacci, de menor a mayor; dicha sucesión se obtiene de la siguiente manera:

1 – 2 – 3 – 5 – 8 – 13 – 21 – 34 – N

Dónde:

N, es el siguiente número en la serie, el cual es calculado con la suma de los dos valores anteriores. Dicha asignación de valores permite identificar cuáles son los tipos de impactos con mayor y menor prioridad.

Los tipos de impacto serán asociados y desglosados en cada subproceso, para los cuales será asignado un valor (4, 3, 2, 1), el cual nos dará como resultado de la siguiente formula el total del impacto:

$$\text{TOTAL DE IMPACTO} = (F1 \times V) + (F2 \times V) + (F3 \times V) \dots + (Fn \times V)$$

Donde:

F, numero de la serie de Fibonacci asignado al tipo de impacto.

V, numero asignado al nivel de afectación (Muy alto–4, Alto–3, Medio–2, Bajo–1).

La sumatoria de la serie de Fibonacci sirve para determinar el total de impacto y evaluar los límites mencionados:

SEVERIDAD	RANGO
ALTA	35 - 44
MEDIA	23 – 34
BAJA	11 – 22

- Punto Objetivo de Recuperación (RTO)**

El RTO al igual que el valor total de impacto, será determinado mediante los siguientes niveles:

Nivel RTO	Horas
CORTO	Menor a 24
MEDIO	De 24 a 48
AMPLIO	Mayor a 48

Tomando en consideración que se manejaran los tiempos en horas naturales (24 horas, 1 día) el RTO estará parametrizado para definir el nivel de criticidad de cada uno de los servicios, procesos o actividades.

De la combinación de la relevancia por tipo de impacto y nivel de RTO resultan 3 posibles clasificaciones para el nivel de criticidad:

		RTO (Tiempo Objetivo de Recuperación)		
		Amplio	Medio	Corto
Valor total del impacto	Alto	Importante	Crítico	Crítico
	Medio	Necesario	Importante	Crítico

	Bajo	Necesario	Necesario	Importante
--	------	-----------	-----------	------------

Nivel de Criticidad	Descripción
Crítico	Alto impacto en la provisión de sus servicios. El impacto se manifiesta en un muy corto plazo después de una interrupción, por lo que su tiempo de recuperación debe ser en término de horas.
Importante	Menor impacto en la provisión de sus servicios. El impacto no se manifiesta en un corto plazo después de una interrupción, por lo que su tiempo de recuperación puede estar en términos de días.
Necesaria	Bajo impacto en la provisión de sus servicios. El impacto se manifiesta en un largo plazo después de una interrupción, por lo que su tiempo de recuperación puede estar en términos de días, semanas o incluso en meses.

- b) **Análisis y consolidación:** Tomando los resultados obtenidos dentro de las sesiones para la recopilación de información con los dueños de los productos/servicios, procesos o actividades, se consolidará la información en un Informe de Resultados de Análisis de Impacto al Negocio y de Riesgos, toda la información recopilada.
- c) **Aprobación de los resultados del BIA por la Alta Dirección:** Una vez obtenida toda la información relacionada a los requerimientos por parte de la empresa, se procederá a la revisión y aprobación por la Alta Dirección, esto con la finalidad de robustecer y empoderar los resultados obtenidos en las sesiones de trabajo.

5. METODOLOGÍA PARA EL ANÁLISIS DE IMPACTO A LAS APLICACIONES

La metodología que tomará como insumo las aplicaciones identificadas como necesarias para la ejecución de los procesos sustantivos identificados dentro del Análisis de Impacto al Negocio (BIA), se muestra en la siguiente figura. Posteriormente, se realizarán entrevistas con los dueños de las aplicaciones y responsables de los procesos relacionados con las mismas para identificar impactos y tiempos de recuperación objetivo, para acordar una secuencia de recuperación en caso de presentarse un incidente de acuerdo con las necesidades de la empresa para la ejecución del servicio, la cual toma como referencia las mejores prácticas

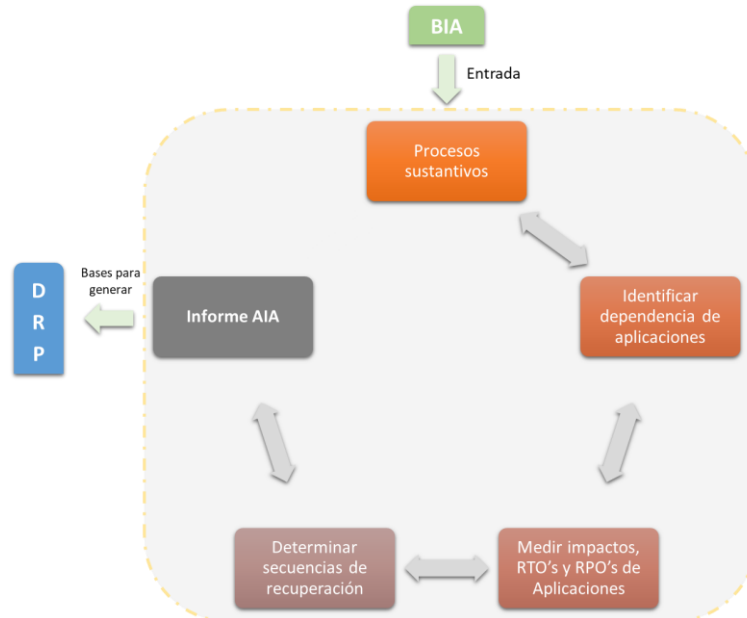


Figura. 2 Metodología Análisis de Impacto a los Aplicativos



Figura. 7 Modelo de levantamiento y análisis de información.

Los objetivos del AIA son los siguientes:

- **Evaluación de niveles de impacto en las aplicaciones** identificadas como críticas con base en el análisis de las relaciones que tienen con los procesos sustantivos de la empresa, conforme a los Escenarios de Riesgo:

ESCENARIOS DE RIESGO
Desastres Naturales y Ambientales
Ataques cibernéticos o a la actividad informática
Sabotaje
Terrorismo
Interrupción en el suministro de energía
Fallas o indisponibilidad en la infraestructura tecnológica (telecomunicaciones, procesamiento de información y redes)
Indisponibilidad de recursos humanos, materiales o técnicos
Interrupción en servicios prestados por terceros

El impacto es el efecto causado en la empresa por la falta de disponibilidad en las aplicaciones.

Para determinar el nivel de impacto en el caso de una interrupción en las aplicaciones, se han considerado al menos los tipos de impacto que se detallan en la siguiente tabla:

TIPOS DE IMPACTO
Operacional
Regulatorio o Normativo
Afectación en la Imagen, Reputacional

TIPOS DE IMPACTO	SEVERIDAD	DESCRIPCIÓN
Afectación operacional	MUY ALTA	Suspende la operación o genera afectación a más de un proceso sustantivo de la empresa
	ALTO	Genera afectación a un proceso sustantivo de la empresa
	MEDIO	Genera afectación a uno o más procesos de soporte para la empresa.
	BAJO	Suspende la operación o genera reprocesos menores a 4 horas.

TIPOS DE IMPACTO	SEVERIDAD	DESCRIPCIÓN
Impacto Regulatorio o Normativo	MUY ALTO	Podrían generarse penalizaciones, y/o investigación contra la empresa por faltas a normatividad Nacional o Constitucional.
	ALTO	Podrían generarse penalizaciones y/o investigación contra la empresa n por faltas a los organismos reguladores (SAT, STPS, PROFECO, LFPDPPP, CONDUSEF, etc.)
	MEDIO	Faltas a los procedimientos, políticas manuales y/o reglamentos organizacionales.
	BAJO	Sin afectación regulatoria o normativa.
Afectación en la Reputación / Imagen Pública o Política	MUY ALTO	Cobertura mediática nacional y limitada a nivel internacional, pérdida seria de clientes, investigación formal del regulador, implicación de directivos.
	ALTO	Cobertura mediática a escala nacional, incremento en reclamaciones de clientes, pérdida de clientes, solicitud de información del regulador (informal).
	MEDIO	Cobertura mediática local o del sector, reclamaciones de clientes, posible pérdida de clientes.
	BAJO	Sin cobertura mediática o efecto externo.

- **Evaluación de la criticidad**

El valor total del impacto estará dado en las siguientes categorías:

SEVERIDAD	VALOR
MUY ALTO	4
ALTO	3
MEDIO	2
BAJO	1

Para determinar los límites de los impactos, de acuerdo con su tipo le será asignado un número de acuerdo con la sucesión de Fibonacci, de menor a mayor; dicha sucesión se obtiene de la siguiente manera:

1 – 2 – 3 – 5 – 8 – 13 – 21 – 34 – N

Donde:

N, es el siguiente número en la serie, el cual es calculado con la suma de los dos valores anteriores. Dicha asignación de valores permite identificar cuáles son los tipos de impactos con mayor y menor prioridad.

Los tipos de impacto serán asociados y desglosados en cada subproceso, para los cuales será asignado un valor (4, 3, 2, 1), el cual nos dará como resultado de la siguiente formula el total del impacto:

$$TOTAL DE IMPACTO = (F1 \times V) + (F2 \times V) + (F3 \times V) \dots + (Fn \times V)$$

Donde:

F, número de la serie de Fibonacci asignado al tipo de impacto.

V, número asignado al nivel de afectación (Muy alto–4, Alto–3, Medio–2, Bajo–1).

La sumatoria de la serie de Fibonacci sirve para determinar el total de impacto y evaluar los límites mencionados:

SEVERIDAD	RANGO
ALTA	18 - 24
MEDIA	12 – 17
BAJA	6 – 11

- **Identificar los RTO's y RPO's por cada aplicación.**

El **tiempo objetivo de recuperación (RTO)** es el tiempo que se puede tolerar la falta de funcionamiento de las aplicaciones y la caída del nivel de servicio asociada, sin que se ponga en riesgo la continuidad de la operación.

El RTO al igual que el valor total de impacto, será determinado mediante los siguientes niveles:

Nivel RTO	Horas
CORTO	Menor a 24
MEDIO	De 24 a 48
AMPLIO	Mayor a 48

Tomando en consideración que se manejan los tiempos en horas naturales (24 horas, 1 día) el RTO estará parametrizado para definir el nivel de criticidad de cada una de las aplicaciones. De la combinación de la relevancia por tipo de impacto y nivel de RTO resultan 3 posibles clasificaciones para el nivel de criticidad:

		RTO (Tiempo Objetivo de Recuperación)		
		Amplio	Medio	Corto
Valor total del impacto	Alto	Importante	Crítica	Crítica
	Medio	Necesaria	Importante	Crítica
	Bajo	Necesaria	Necesaria	Importante

Nivel de Criticidad	Descripción
Crítica	Alto impacto en la provisión de sus servicios. El impacto se manifiesta en un muy corto plazo después de una interrupción, por lo que su tiempo de recuperación debe ser en término de horas.
Importante	Menor impacto en la provisión de sus servicios. El impacto no se manifiesta en un corto plazo después de una interrupción, por lo que su tiempo de recuperación puede estar en términos de días.
Necesaria	Bajo impacto en la provisión de sus servicios. El impacto se manifiesta en un largo plazo después de una interrupción, por lo que su tiempo de recuperación puede estar en términos de días, semanas o incluso en meses.

- El **punto objetivo de recuperación (RPO)** es el volumen de datos en riesgo de pérdida que las áreas consideran tolerables en una situación de desastre. Generalmente va en función del tiempo de realización de los respaldos o sincronización de los datos.
- **Determinar la secuencia de recuperación de las aplicaciones** con base en los tiempos objetivos de recuperación (RTO's), así como su criticidad.
 La secuencia de recuperación servirá como insumo para la generación y posterior detonación del DRP de la empresa.

- **Identificar periodos críticos de uso por aplicación (meses, días y horas).** Los periodos críticos de las aplicaciones se refieren al uso que tienen durante el transcurso del año derivado de las cargas de trabajo, por día, mes, año y horarios. Esto con la finalidad de identificar los “picos” y las temporadas en que la interrupción del servicio puede volverse aún más crítico.
- **Obtener las interempresas entre las aplicaciones sustantivas de la empresa.**

Una interempresa significa que alguna aplicación requiere de una u otras aplicaciones para poder funcionar correctamente, ya sea porque comparten la misma base de datos o se requiera acceder a información de ese sistema.

6. Anexos

NA