RIESGOS Y ANÁLISIS DE IMPACTO AL NEGOCIO (BIA)

Objetivo:

Conocer cómo se identifican y evalúan los riesgos y su impacto en los procesos.

Contenido:

- ✓ ¿Qué es un Análisis de Riesgos?
- ✓ ¿Qué es un Análisis de Impacto al Negocio (BIA)?
- ✓ Ejemplos de escenarios disruptivos relevantes para la Cooperativa
- ✓ Resultados clave del BIA de la entidad (ej. procesos críticos)

¿QUÉ ES UN ANÁLISIS DE RIESGOS?

Un análisis de riesgos es un proceso sistemático para identificar, evaluar y priorizar las amenazas que podrían afectar negativamente a una organización o a una actividad. Su objetivo es prever esos riesgos, estimar su probabilidad e impacto, y así desarrollar planes de acción para mitigar sus consecuencias y tomar decisiones informadas.

La Cooperativa ha elaborado el Análisis de Riesgos de Seguridad de Información, el cual de acuerdo a la metodología seleccionada ha identificado las Amenazas y Vulnerabilidades, estimando su Riesgo Inherente, Riesgo Residual y determinando mitigadores con respecto a la falta o degradación de la confidencialidad, integridad o disponibilidad de los Activos de información.

De manera complementaria se ha realizado el análisis de riesgos de acuerdo a su manifestación que podrían afectar la CONTINUIDAD DEL NEGOCIO, tales como: **Desastres Naturales, Daño Accidentales** y **daños Intencionales**, enfocados tanto a la Oficina Central como a la Agencia, para lo cual se ha planteado algunos escenarios donde el resultado en la tabla derecha:

Desastres Naturales	Sismo / Terremoto	Riesgo Bajo
Desastres Naturales	Tormenta eléctrica	Riesgo Bajo
Daños Accidentales	Incendios	Riesgo Medio
Desastres Naturales	Inundación	Riesgo Bajo
Daños Accidentales	Fallo de suministro eléctrico	Riesgo Medio
Daños Accidentales	Falla Tecnológica	Riesgo Medio
Desastres Naturales	Pandemia / Epidemia	Riesgo Bajo
Daño intencional	Ciberataque	Riesgo Alto

¿Qué es un Análisis Impacto del Negocio?

El Análisis BIA se convierte en una herramienta para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afectan las operaciones regulares, por lo consiguiente debe formar parte de un sistema de gestión de riesgos, que sea utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.

La Cooperativa ha implementado su Análisis BIA de acuerdo a los siguientes objetivos:

- ✓ Determinar los procesos y actividades críticas que garantizan la continuidad de las operaciones de la Cooperativa y los posibles impactos que se tendrían si éstos no se encuentran disponibles y operables.

- ✓ Estimar los tiempos objetivos de recuperación de los procesos y actividades críticas con el fin de restaurarlos a su operación normal después que ha ocurrido un desastre o evento disruptivo y los tiempos requeridos para disminuir la pérdida de datos.

REQUERIMIENTO DE TIEMPOS DE RECUPERACIÓN:

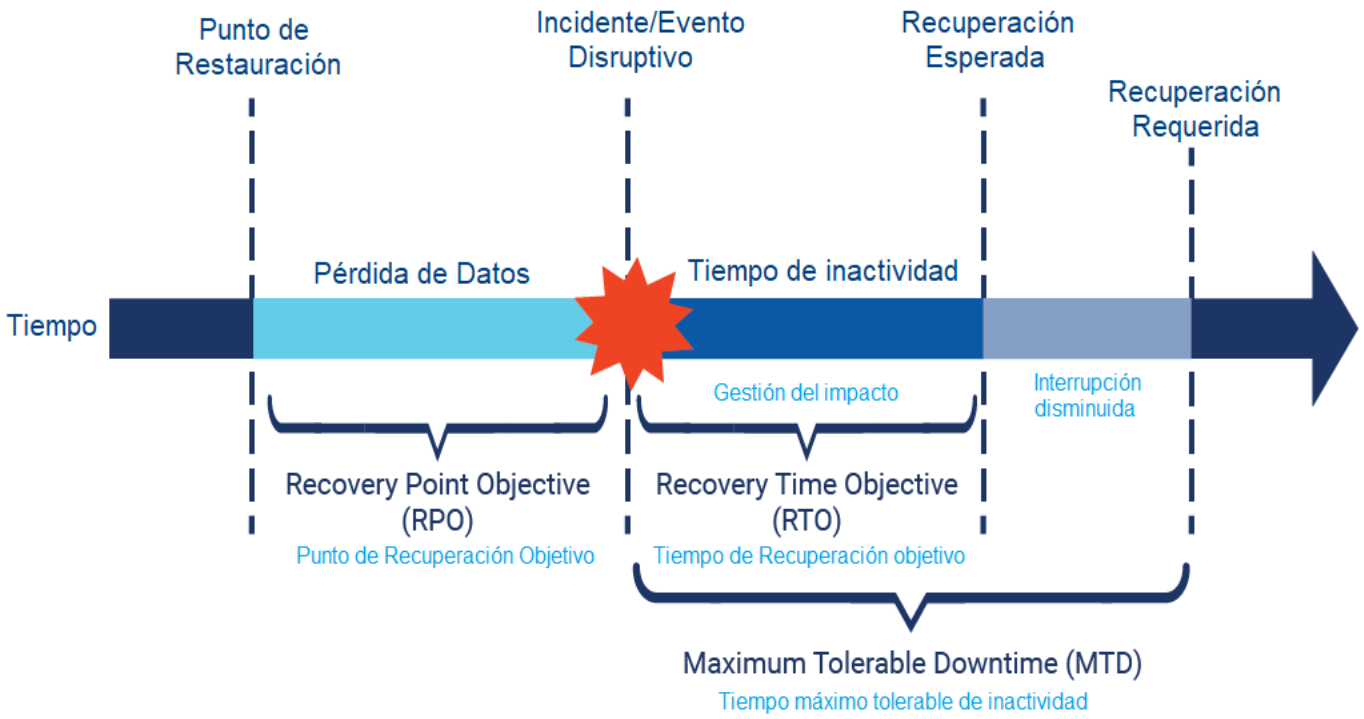
Es importante definir y entender los requerimientos de tiempo necesarios para recuperar los servicios que han sido interrumpidos por diferentes motivos; estos requerimientos obedecen a varios componentes que hacen referencia concreta al tiempo disponible en la cual una organización puede recuperarse oportuna y ordenadamente a las interrupciones en los servicios e infraestructuras de TI. Estos componentes se describen como indicadores y son:

- ✓ **MTD** (**Maximun Tolerable Downtime**) o Tiempo Máximo de Inactividad Tolerable. Espacio de tiempo durante el cual un proceso puede estar inoperante hasta que la empresa empiece a tener pérdidas y colapse.

- ✓ **RTO** (**Recovery Time Objective**) o Tiempo de Recuperación Objetivo. Es el tiempo transcurrido entre una interrupción y la recuperación del servicio. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

- ✓ **RPO** (**Recovery Point Objective**) o Punto de Recuperación Objetivo. Es el rango de tolerancia que la entidad puede tener sobre la pérdida de datos y el evento de desastre.

La siguiente imagen describe gráficamente los pasos para realizar el análisis de impacto. También esta conceptualización se sustenta en la **ISO 22313**.



IDENTIFICACIÓN DE LOS PROCESOS CRÍTICOS:

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de la Cooperativa según los niveles de impacto. A continuación, se identifican algunas que han sido clasificados como críticas que en caso de un evento disruptivo se deben tomar prioridad:

No.	ÁMBITO	PROCESO	SUB PROCESO
1	NEGOCIO	Administración de **CAPTACIONES**	Registro de transacciones de Depósito/Retiro/Pago de Crédito
2			Apertura/Traspaso/Arqueo en Cajas
3			Apertura y Traspaso y Cierre de Bóveda
4			Transporte de Material Monetario
5			Banca Móvil
6			Envío periódico de información a ASFI y BCB
7		Administración de **CRÉDITOS**	Análisis, Evaluación y Determinación de capacidad de pago
8			Control de Mora y Recuperación
9			Envío periódico de información a ASFI (CIC y otros diarios)
10	CORPORATIVO	Administración de TI	Administración de Información Tecnológica.
11			Administración de los Sistemas de Información (SFI, SAI)
12			Administración de la Banca Electrónica
13			Administración de la Red y comunicación (Central y Agencia)
14			Administración de Servidores CPD y CPDA
15			Gestión de Soporte a Estaciones de Trabajo
16			Gestión de SLA con Soporte Tercerizados en TI
17		Administración Institucional	Administración de los Bienes e Instalaciones Físicas.
18		Administración Contable y RR.HH.	Administración de Recursos Humanos.
19			Gestión de Proveedores y Servicios Tercerizados.
20			Envío mensual, semanal y diario de información a ASFI por SCIP
21		Gestión de riesgo Integral	Envío de información semanal y Trimestral a ASFI
22		Investigación financiera	Gestión de Registros de Operaciones Sospechosas
23			Envío periódico de Información a ASFI y la UIF.
24		Gestión de Seguridad Física	Control de Monitoreo de Vigilancia de Seguridad
25		Gestión de la Seguridad de Información	Gestión de la Seguridad de Información
26			Gestión de Incidentes de Seguridad de la Información
27			Gestión del Plan de Continuidad del Negocio

IDENTIFICACIÓN DE LOS PROCESOS ALTERNOS:

Actualmente la Cooperativa cuenta con los siguientes procesos alternos que son activados en caso de irrupciones o eventos que afecten la Continuidad del Negocio:

a) Centro de Procesamiento de Datos Alterno (CPDA)

Un centro de procesamiento de datos alterno (CPDA), también llamado centro de respaldo, es una **instalación secundaria** y estratégicamente ubicada que funciona como una copia de seguridad de un centro de procesamiento de datos principal (CPD). Su propósito es asegurar la continuidad del negocio y la disponibilidad de datos en caso de desastres, fallos técnicos o ciberataques en el sitio primario.

La Cooperativa, cuenta con el Centro de Procesamiento de Datos Alterno, ubicado en la Agencia Mercado Campesino, la misma cumple con todos los aspectos exigidos por la normativa. Su infraestructura está compuesta por todos los recursos necesarios como Energía, Red, climatización, seguridad física, etc., para tomar el control en caso de que el CPD principal no esté operativo. Periódicamente, se realizan pruebas de Activación del CPDA.

b) Contingencia Operativa Manual

Una contingencia operativa manual es un plan de respaldo que se ejecuta sin el uso de sistemas automatizados cuando ocurre un problema inesperado, como una falla eléctrica o del sistema informático. Consiste en un conjunto de procedimientos y recursos predefinidos que se ponen en marcha para continuar las operaciones críticas de la forma más rápida posible.

Se ha implementado un Plan de contingencia Operativa Manual para la Oficina central y la Agencia respectivamente, donde se han definido los responsables de su activación, especificando una matriz de roles para tal efecto. En el documento de Plan de Contingencia Operativo Manual, define un procedimiento, para lo cual la estrategia adoptada se describe de la siguiente manera:

ANTES:

Antes de la interrupción total del Servicio a los Socios(as), se debe prever y contar con:

- Backup del Sistema SFI
- Disponibilidad de CPDA (Infraestructura Tecnológica)
- Plan de Contingencia Operativa
- Personal capacitado en la ejecución del Plan de contingencia operativa manual.

DURANTE:

Durante el suceso se debe tomar en cuenta las necesidades de los consumidores financieros:

A) Activación del Plan de Continuidad del Negocio / Plan de contingencia Tecnológica
B) Atención al cliente/socio en plataforma de manera manual o semi manual
C) Atención en Caja e manera manual o semi manual

DESPUÉS:

1) Comunicar la Desactivación del proceso manual.
2) Se realiza el Backup del Sistema
3) Se migra el Backup del CPDA al CPD Principal
4) Se desactiva el CPDA
5) Se restaura el Backup en el SERVIDOR PRINCIPAL.
6) Registrar todos los recibos realizados de transacciones en la oficina central bajo la supervisión de la jefe Comercial y Captaciones, quienes validaran la información procesada. En el caso de la Agencia, será bajo la supervisión de la Encargada de Agencia y/o Captaciones quienes validarán la información procesada.
7) Una vez registrado, se debe validar la integridad de la información registrada.
8) Se comunicará a todas las áreas el inicio normal de todos los servicios y procesos de la entidad.
9) El equipo de veedores de todo el proceso manual debe reunirse y realizar un análisis de los procedimientos para considerar posibles ajustes.
10) Se debe registrar el suceso como INCIDENTE DE SEGURIDAD DE INFORMACIÓN y considerarlo como EVENTO DE RIESGO OPERATIVO.
11) Emitir un informe detallado del procedimiento aplicado.