PIC

Programa Integral de Capacitación en Gestión de Riesgos 2025

RIMAC | fri·esan Finance & Regulation Institute

PIC

Programa Integral
de Capacitación

Ciclo V

Prevención ante Situaciones de
Emergencia y Desastres

Tema: Continuidad de Negocio según ISO 22301

RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

En RIMAC las personas van primero

Nos hemos propuesto construir relaciones a largo plazo con las personas que se acercan a nosotros.

RIMAC

fri·esan
Finance & Regulation Institute

Ing. Raúl Díaz

Ph.D.(c) Candidato a doctor en Gestión Estratégica en el Consorcio de Universidades del Perú. Magister en Administración de Negocios con mención en Finanzas Corporativas en ESAN. Ingeniero de Sistemas de la Universidad de Lima. Socio Líder de Consultoría de Strategos Consulting Services con más de 17 años de experiencia en servicios de consultoría y capacitación en Latinoamérica sobre transformación digital, ciberseguridad, riesgos, continuidad de negocios y prevención del fraude en la industria de tarjetas de pago, banca, energía, salud y gobierno.

RIMAC

PIC
Programa Integral
de Capacitación

Agenda

- Introducción
- Análisis de impacto al negocio
- Gestión de riesgos de continuidad
- Estrategias de continuidad del negocio

RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

1. Introducción

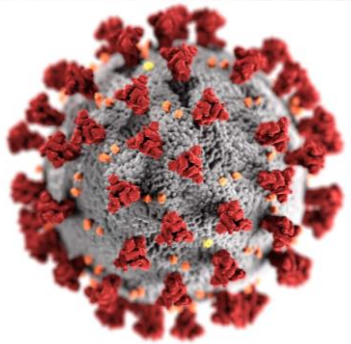
RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

Incidentes que pueden afectar la Continuidad del Negocio

- Percepción negativa del público hacia la organización
- Problema con productos y servicios
- Problema financiero
- Problema de relaciones con empleados
- Evento internacional adverso
- Violencia en el lugar de trabajo
- Pérdida de personal
- Desastre natural



RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

Amenazas cibernéticas



Políticas	•Políticas especificas de seguridad
Red Externa	•Firewall perimetral / Firewall de aplicación •Balanceador / CASB Nube
Seguridad física	•Vigilancia, Acceso
Red Interna	•Firewall interno, Monitoreo de red, Sistema de Prevención de Intrusos
Aplicaciones	•Codificación Segura •Analizador de vulnerabilidades (SAST, DAST)
Sistema operativo	•Privilegios de usuario •Antivirus, Antimalware, Configuraciones seguras
Datos	•Firewall de datos

RIMA

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

Video de Continuidad de Negocio

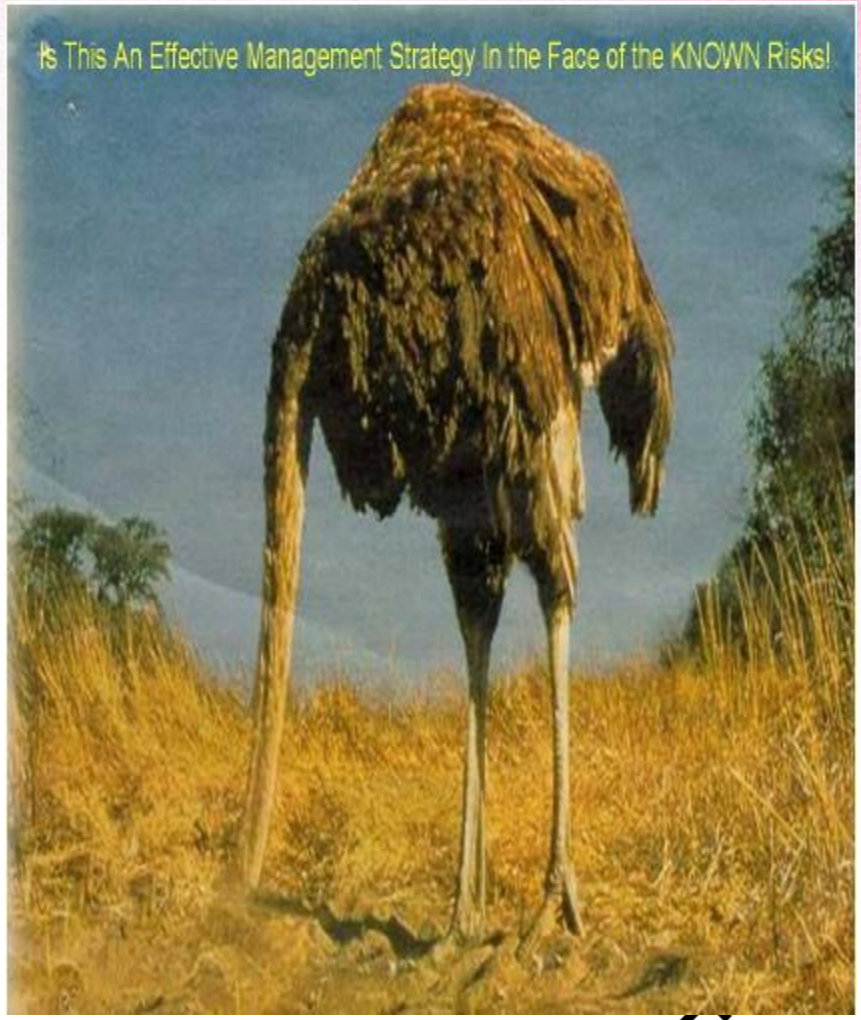
RIMAC

fri·esan
Finance & Regulation Institute

Programa Integral de Capacitación

Lo anterior es cierto, pero …

- “Nosotros somos inmunes a desastres”
- “Eso nunca pasará aquí”
- “Nosotros tenemos una política de seguros, eso es suficiente”
- “Nosotros nunca hemos
- tenido problemas antes”



Programa Integral de Capacitación

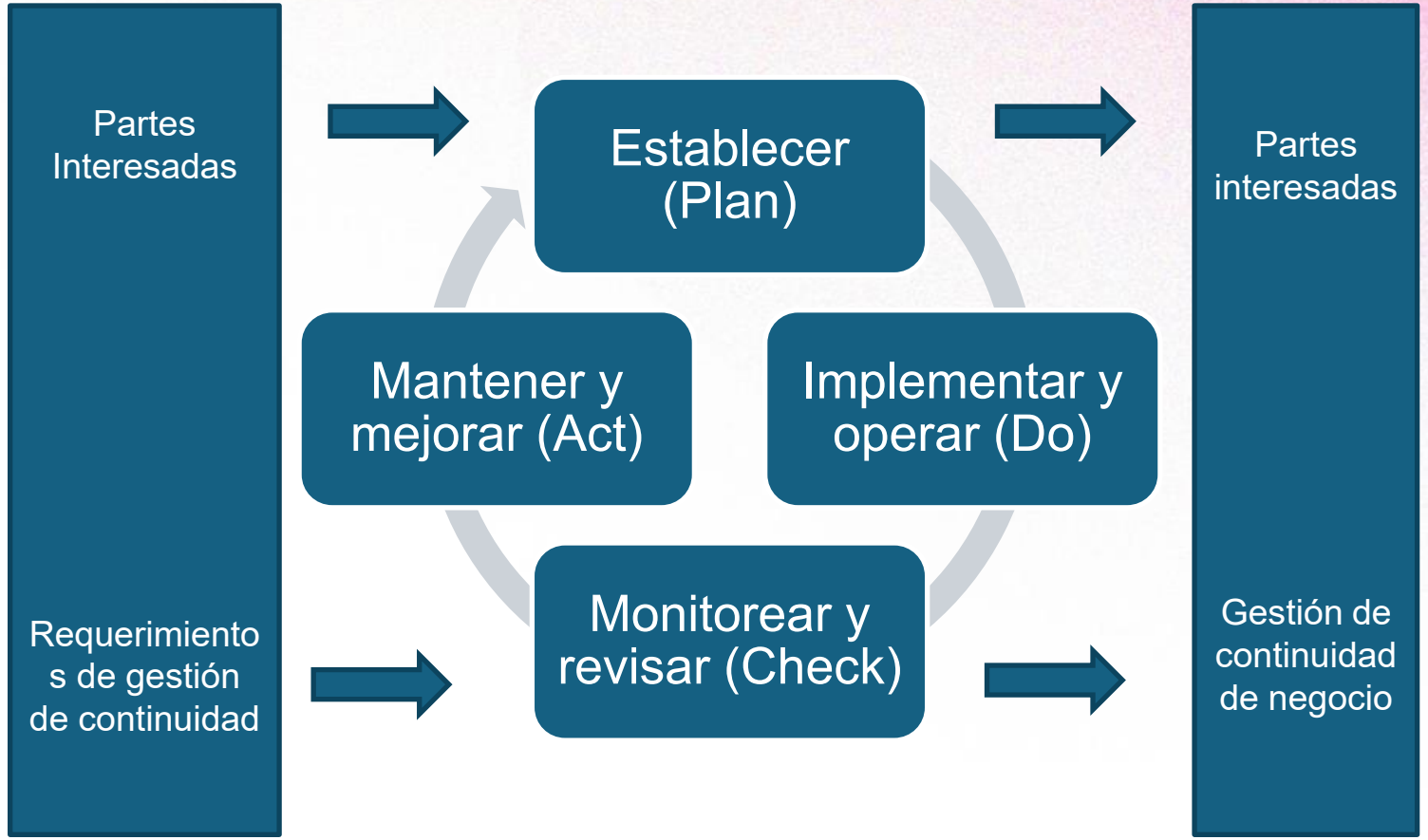
Conceptos generales

- **Actividad:** conjunto de una o más tareas con un resultado definido.
- **Auditoria:** proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla determinar objetivamente en qué medida se cumplen los criterios de auditoría.
- **Continuidad de negocio:** capacidad de una organización para continuar la entrega de productos y servicios dentro marcos de tiempo aceptables a una capacidad predefinida durante una interrupción.
- **Plan de continuidad de negocio:** información documentada que guía a una organización para responder a una interrupción y reanudar, recuperar y restablecer la entrega de productos y servicios en consonancia con su negocio continuidad objetivos.
- **Acción correctiva:** acción para eliminar la(s) causa(s) de una no conformidad y para prevenir la recurrencia.
- **Disrupción:** incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización.
- **Información documentada:** información requerida para ser controlada y mantenida por una organización y el medio en que está contenido.

Programa Integral de Capacitación

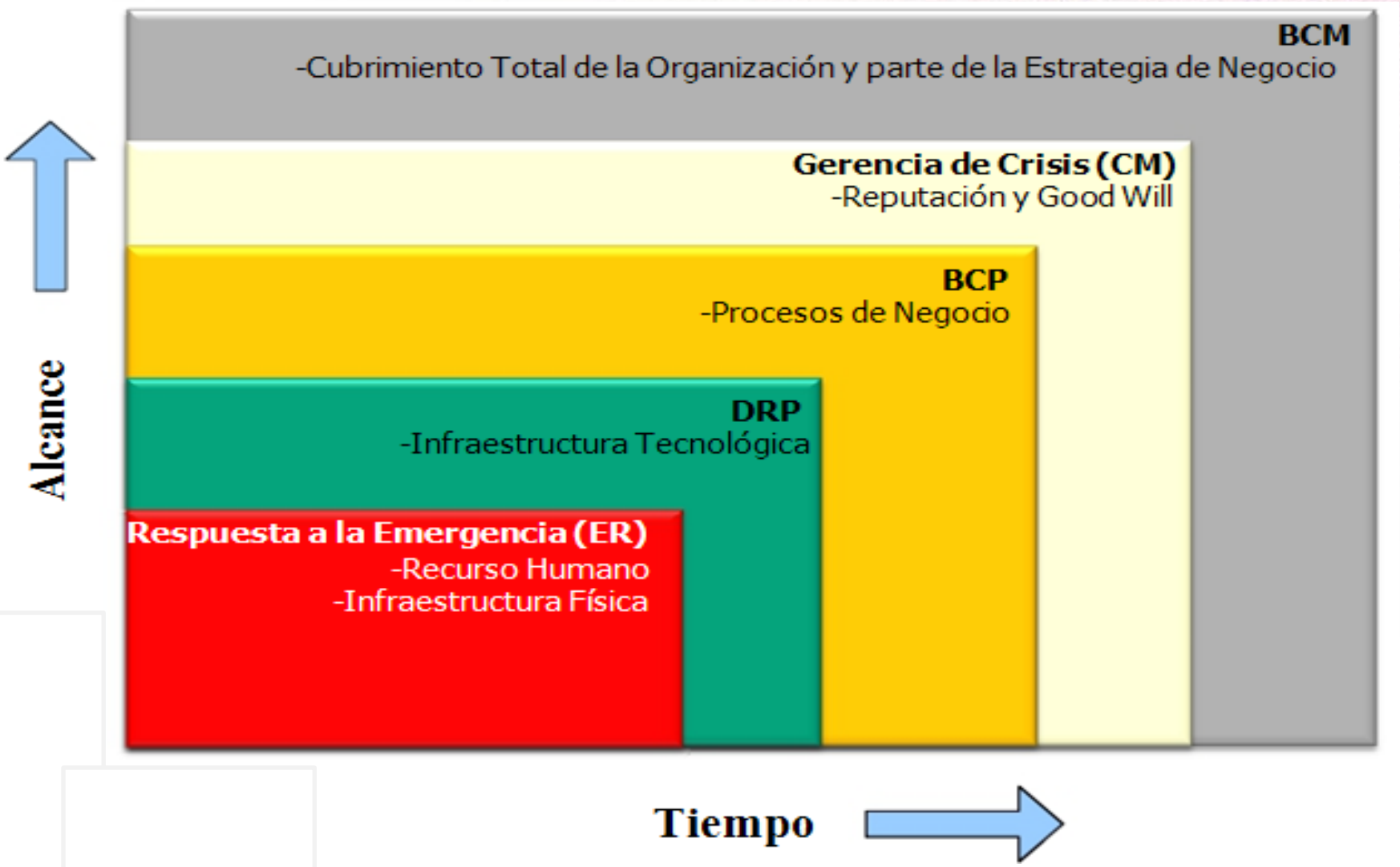
PDCA de un Sistema de Continuidad de Negocio

- Este ciclo mejora la efectividad del sistema de gestión de continuidad de negocio según la ISO/IEC 22301:2019
- Este ciclo se alinea a las normas ISO/IEC 14001, ISO/IEC 20000-1, ISO/IEC 27001, ISO/IEC 28000 e ISO/IEC 9001.



Programa Integral
de Capacitación

Evolución del SGCN



Programa Integral de Capacitación

Estructura de la ISO/IEC 22301

4. Contexto de la organización

- Entendimiento de la organización y su contexto
- Entender las necesidades y expectativas de las partes interesadas
- Determinar el alcance del SGCN
- SGCN

5. Liderazgo

- Liderazgo y compromiso
- Política
- Roles y responsabilidades

6. Planificación

- Acciones de evaluación de riesgos y oportunidades
- Objetivos de continuidad de negocio
- Planificación de cambios del sistema de continuidad de negocio

7. Soporte

- Recursos
- Competencias
- Concientización
- Comunicación
- Información documentada

8. Operación

- Planificación operacional y control
- Análisis de impacto al negocio y Evaluación del riesgo
- Plan de continuidad de negocio y procedimientos
- Programa de ejercicios
- Evaluación de la documentación de la continuidad del negocio y capacidades

9. Evaluación

- Monitoreo, análisis y evaluación
- Auditoria interna
- Revisión de la gestión

10. Mejora

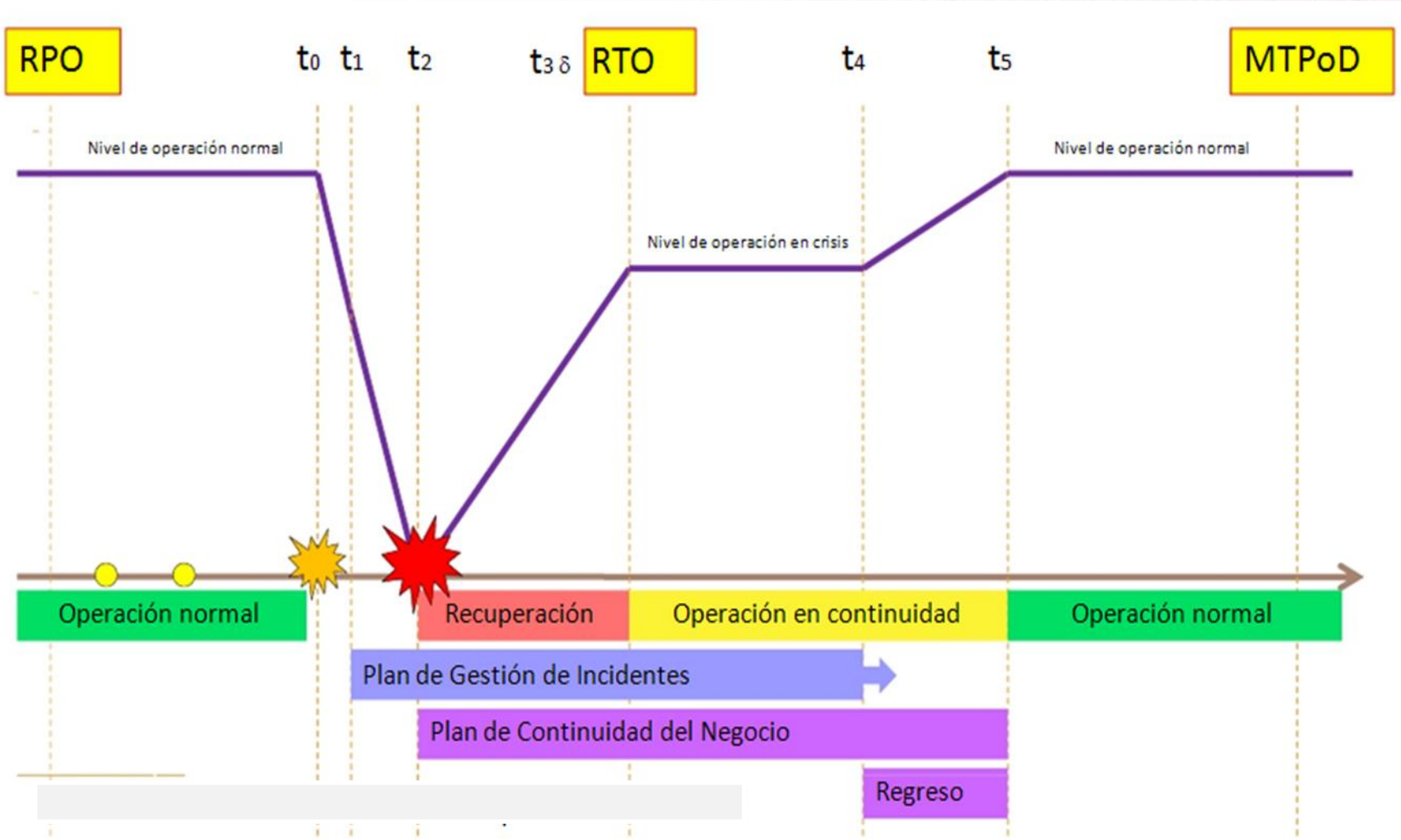
- No conformidad y acción correctiva
- Mejora continua

RIMAC

fri·esan Finance & Regulation Institute

Programa Integral
de Capacitación

Tiempos de recuperación



PIC
Programa Integral
de Capacitación

Descripción de los tiempos de recuperación

- **MTD (Maximum Tolerable Downtime):** Este tiempo representa el periodo máximo de tiempo de inactividad que puede tolerar la organización, sin entrar en un colapso financiero y operacional.
- **RTO (Recovery Time Objective):** Indica el tiempo disponible para recuperar sistemas y/o recursos que han sufrido una alteración.
- **RPO (Recovery Point Objective):** Se refiere a la magnitud de la pérdida de datos, medida en términos de un periodo de tiempo que un proceso de negocios puede tolerar.
- **WRT (Work Recovery Time):** Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas estén reparados, dentro del **MTD**.

La suma de los tiempos del **RTO** y **WRT** serán iguales o menores que el **MTD**. Jamás pueden ser mayores.

RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

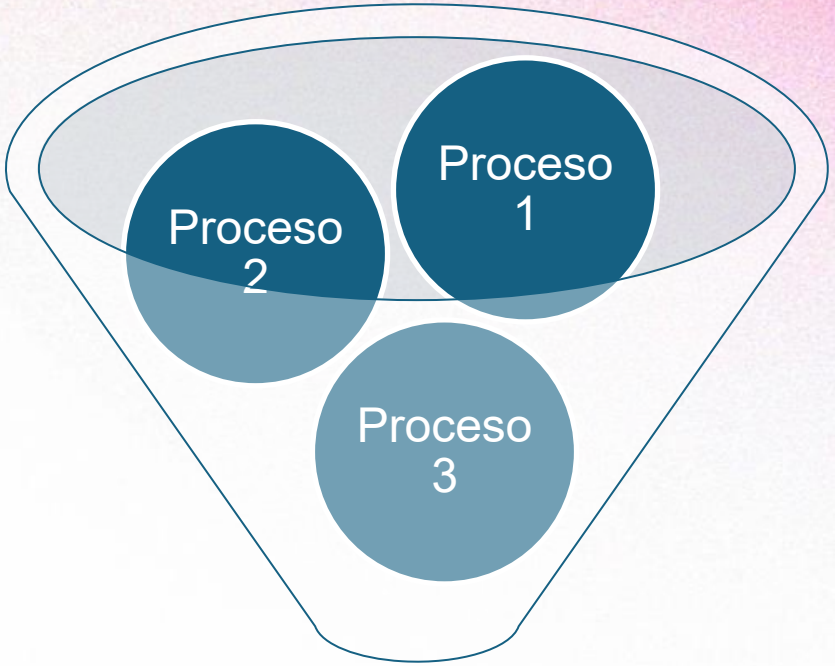
2. Análisis de Impacto al Negocio

RIMAC

fri·esan
Finance & Regulation Institute

Análisis de Impacto al Negocio (BIA)

- Se usa para determinar los procesos críticos y los recursos relacionados dentro de todas las unidades de negocios de la organización.
- Establece una base para desarrollar respuestas bien fundamentadas y priorizadas al desastre y asegura que los planes de continuidad del negocio estén enfocados en restablecer los procesos comerciales más críticos de la manera más rentable para minimizar la pérdida y la interrupción.
- El objetivo del BIA es definir los objetivos para la recuperación de los dispositivos que soportan los sistemas informáticos que ejecutan las aplicaciones de procesos críticos; específicamente, los objetivos se definen en número de horas o días en que los sistemas deben recuperarse después de una interrupción.



Análisis de Impacto al Negocio (BIA)

Programa Integral de Capacitación

Análisis de Impacto al Negocio

N°	Proceso / Actividad	Impacto Operativo	MTD	RTO	WRT	RPO	Recursos Críticos

PIC
Programa Integral
de Capacitación

Taller 1: Análisis de Impacto al Negocio (BIA) – 30 minutos

- Realiza un análisis de impacto al negocio para un proceso de tu negocio.

RIMAC

fri·esan
Finance & Regulation Institute

PIC
Programa Integral
de Capacitación

3. Gestión de Riesgos de Continuidad

RIMAC

fri·esan
Finance & Regulation Institute

Programa Integral
de Capacitación

Gestión de riesgos según ISO 31000

Principios

1. Crear valor.
2. Parte integral de los procesos de la organización.
3. Parte de la toma de decisión.
4. Trata explícitamente las incertidumbres.
5. Sistemática, estructurada y oportuna.
6. Basada en la mejor información disponible.
7. Hecha a medida.
8. Tiene en cuenta factores humanos y culturales.
9. Transparente e inclusiva.
10. Dinámica, interactiva y capaz de reaccionar ante los cambios.
11. Permite la mejora continua de la organización.

Marco de referencia

Proceso

Programa Integral de Capacitación

Identificación de riesgos

Identificación del riesgo: proceso de encontrar, reconocer y describir riesgos.

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un proceso de negocio o activo. También se conoce como causa de riesgo.

Riesgo: efecto de la incertidumbre sobre conseguir los objetivos.

Dueño del riesgo: persona o entidad con la responsabilidad y autoridad para gestionar un riesgo

Programa Integral de Capacitación

Análisis y Evaluación del riesgo

Análisis de riesgo: proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Evaluación del riesgo: proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable.

Programa Integral de Capacitación

Tratamiento del riesgo

- Tratamiento del riesgo: proceso de modificar el riesgo.

Aceptar: La organización acepta el riesgo porque esta controlado o porque desea aprovecha una oportunidad.	Reducir: La organización decide aplicar medidas que reduzcan el riesgo.
Transferir: La organización comparte el riesgo con un proveedor o adquiere un seguro.	Evitar el riesgo: La organización elimina la actividad de negocio.

Programa Integral de Capacitación

Tratamiento del riesgo

- **Control:** medida que modifica el riesgo
  - Nota 1: Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo.
  - Nota 2: Es posible que los controles no siempre ejerzan el efecto modificador previsto o supuesto.
- **Riesgo residual:** riesgo restante después del tratamiento de riesgo.

Programa Integral de Capacitación

Taller 2: Evaluación de riesgos de continuidad de negocios. (30 minutos)

- Realiza un proceso de evaluación de riesgos de continuidad para uno de tus procesos.

PIC
Programa Integral
de Capacitación

4. Estrategias de Continuidad de Negocio

RIMAC

fri·esan
Finance & Regulation Institute

Programa Integral de Capacitación

Identificación de estrategias

- La identificación se basará en la medida en que las estrategias y soluciones:

a) cumplir con los requisitos para continuar y recuperar las actividades priorizadas dentro de los plazos y capacidad acordada;	b) proteger las actividades prioritarias de la organización;	c) reducir la probabilidad de interrupción;
d) acortar el período de interrupción;	e) limitar el impacto de la interrupción en los productos y servicios de la organización;	f) prever la disponibilidad de recursos adecuados.

RIMAC

fri·esan Finance & Regulation Institute

Programa Integral de Capacitación

Selección de estrategias

- La selección se basará en la medida en que las estrategias y soluciones puedan:

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

RIMAC

fri·esan Finance & Regulation Institute

Programa Integral de Capacitación

Requerimientos de recursos

- La organización debe determinar los requerimientos de recursos para implementar las soluciones de continuidad de negocio seleccionado. Los tipos de recursos considerados incluirán, pero no se limitarán a:

a) una personas;	b) información y datos;	c) infraestructura física como edificios, lugares de trabajo u otras instalaciones y servicios públicos asociados;	d) equipos y consumibles;
e) sistemas de tecnología de la información y la comunicación (TIC);	f) transporte y logística;	g) finanzas;	h) socios y proveedores.

PIC
Programa Integral
de Capacitación

Taller 3: Diseño de estrategias de continuidad de negocios (30 minutos).

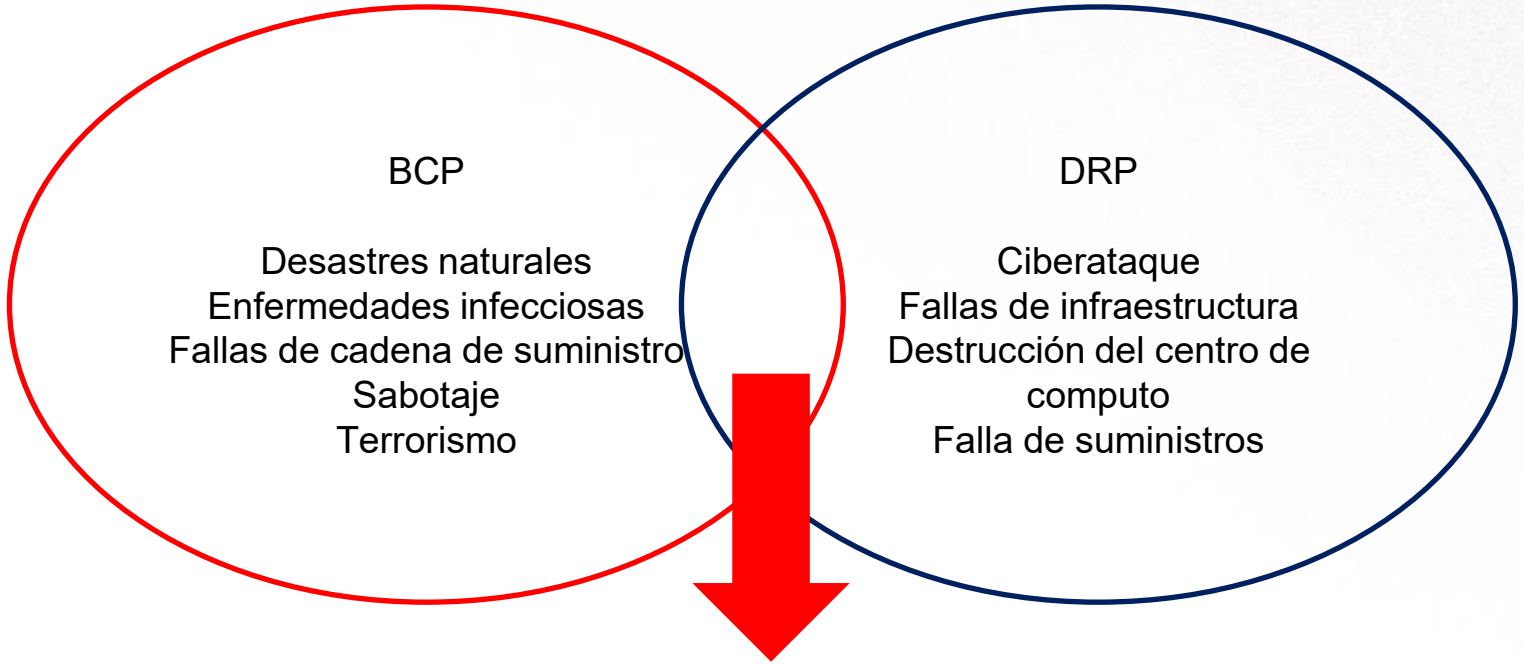
- Realiza una selección de estrategias de continuidad para dos procesos.

RIMAC

fri·esan
Finance & Regulation Institute

Programa Integral de Capacitación

Alineación entre planes BCP y DRP



El negocio debe estar preparado ante la posibilidad de responder a escenarios de contingencias duales considerando que la pandemia ha demostrado que la duración de un evento puede extenderse por periodos de varios meses o incluso años.

PIC
Programa Integral
de Capacitación

¡Gracias!

RIMAC

fri·esan
Finance & Regulation Institute