PIC

Programa Integral de Capacitación en Gestión de Riesgos 2026

RIMAC | fri·esan Finance & Regulation Institute

PIC Programa Integral de Capacitación en Gestión de Riesgos 2026

Tema: Continuidad de Negocio: ISO 22301

RIMAC

fri·esan Finance & Regulation Institute

Dr. Raúl Díaz

Doctor en Gestión Estratégica en el Consorcio de Universidades del Perú. Magíster 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 18 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

Agenda

- Introducción a la norma ISO 22301:2019
- Análisis de contexto y riesgos presentes
- Estructura de un plan de continuidad
- Ciclo de vida del PCN
- Conclusiones

1. Introducción a la ISO 22301:2019

Continuidad de Negocio

- Es la capacidad de una organización para **continuar la entrega de productos y servicios** a niveles **aceptables** tras una interrupción (ISO 22301).


La planificación ayudaría a tu
empresa a recuperarse de...

Amenazas

Ciberseguridad	Tecnología	Energía	Operacional	Regulatorio	Reputacional	Natural	Sanitario
•Ransomware •Phishing / Compromiso de credenciales •Ataque •DDoS •Fuga de información (data breach) •Malware interno	•Caída de proveedor cloud •Falla de servidor crítico •Corrupción o pérdida de base de datos •Fallo en sistemas de respaldo (backup)	•Corte eléctrico prolongado •Falla de UPS o generador	•Ausencia de personal clave •Error humano crítico •Interrupción de proveedor estratégico	•Incumplimiento normativo •Sanción o multa de autoridad supervisora	•Crisis mediática •Publicación de información confidencial	•Terremoto •Inundación •Huaico / deslizamiento •Incendio	•Pandemia

Conceptos generales

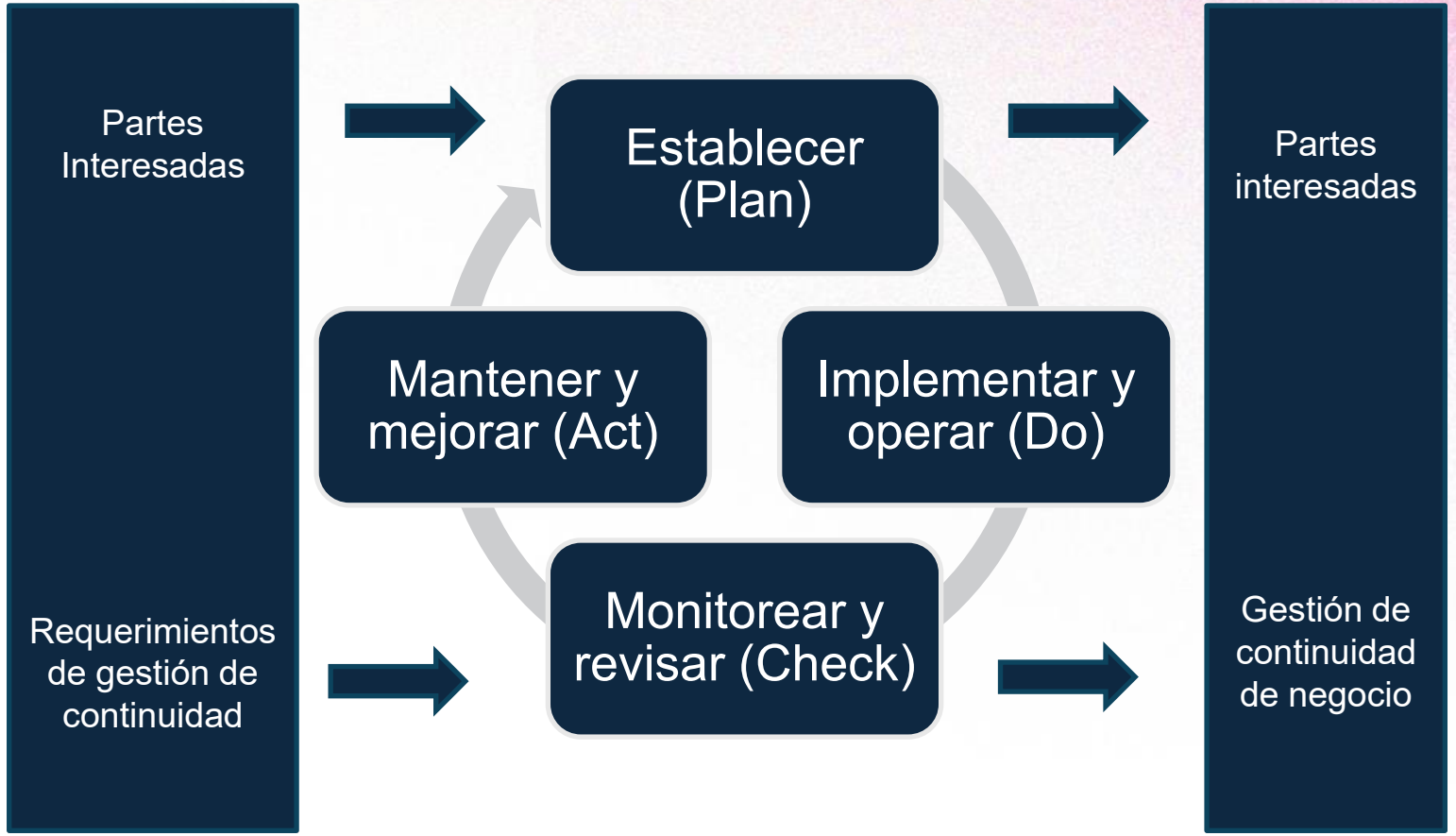
Interrupción	• evento que provoca una desviación negativa no planificada en la operación normal del negocio.
Incidente	• evento que puede convertirse en una interrupción.
Plan de continuidad de negocio	• documento que describe cómo responder a una interrupción y recuperar las actividades críticas.
Análisis de impacto al negocio	• proceso que identifica las actividades críticas, los impactos financieros y operativos, y el tiempo máximo tolerable de interrupción.
Actividad priorizada	• proceso crítico que debe continuar para evitar impactos inaceptables.
Riesgo	• efecto de la incertidumbre sobre los objetivos.
Sistema de Gestión de Continuidad de Negocio (SGCN)	• conjunto estructurado de políticas, procesos y controles para prepararse, responder, recuperarse y mejorar continuamente

Beneficios del SGCN

- Reducción del impacto ante interrupciones: Permite minimizar pérdidas financieras, operativas y legales al contar con planes estructurados de respuesta y recuperación.
- Protección de ingresos y estabilidad financiera: Al mantener operativas las actividades críticas, se evita la paralización total del negocio y la pérdida significativa de ingresos.
- Mayor confianza de clientes y partes interesadas: Demuestra preparación, resiliencia y madurez organizacional, fortaleciendo la reputación y credibilidad institucional.
- Cumplimiento regulatorio y contractual: Facilita el cumplimiento de exigencias normativas y requisitos de clientes, especialmente en sectores regulados (financiero, telecomunicaciones, salud, sector público).
- Mejora de la resiliencia organizacional: Fomenta una cultura de preparación, mejora continua y capacidad de adaptación frente a crisis, aumentando la sostenibilidad a largo plazo.

PDCA de un SGCN

- 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.



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

2. Analisis de Contexto y Riesgos Presentes

Contexto

4.1 Comprensión de la organización y su contexto

- La organización debe:
- Determinar las **cuestiones externas e internas** que sean relevantes para su propósito y que afecten su capacidad para lograr los resultados previstos del SGCN.
- Estas cuestiones deben ser **monitoreadas y revisadas periódicamente**.

Contexto

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

- La organización debe:
  - Determinar las **partes interesadas relevantes** para el SGCN.
  - Determinar sus **requisitos pertinentes**.
  - Identificar cuáles de estos requisitos se convierten en **obligaciones de cumplimiento**.

Contexto

4.3 Determinación del alcance del SGCN

- La organización debe:
  - Determinar los **límites y la aplicabilidad del SGCN**.
  - Considerar:
    - Cuestiones internas y externas (4.1)
    - Requisitos de partes interesadas (4.2)
    - Productos y servicios
  - Definir claramente el alcance como **información documentada**.
  - Indicar exclusiones justificadas, si existen.
  - El alcance debe estar disponible y mantenerse actualizado.

Comprensión de la organización

FORTALEZAS (F)	OPORTUNIDADES (O)
F1. Procesos críticos identificados mediante BIA.	O1. Exigencias regulatorias que impulsan formalización del SGCN.
F2. Compromiso de la Alta Dirección.	O2. Disponibilidad de tecnologías cloud resilientes.
F3. Backups automatizados y documentados.	O3. Ventaja competitiva por certificación ISO 22301.
F4. Integración con gestión de riesgos corporativa.	O4. Acceso a seguros de interrupción del negocio.
F5. Documentación formal del BCP.	O5. Mayor conciencia de ciberseguridad en el mercado.

DEBILIDADES (D)	AMENAZAS (A)
D1. Dependencia de proveedor tecnológico único.	A1. Incremento de ransomware y ciberataques.
D2. Pruebas del BCP no periódicas.	A2. Riesgo sísmico y desastres naturales.
D3. Falta de plan de sucesión formal.	A3. Interrupción de telecomunicaciones.
D4. Cultura organizacional reactiva.	A4. Cambios regulatorios estrictos.
D5. Recursos limitados para sitio alterno.	A5. Crisis reputacional digital.

Comprensión de la organización

Tipo de Estrategia	Acciones Estratégicas
FO (Fortalezas + Oportunidades)	• Utilizar infraestructura existente para lograr certificación ISO 22301. • Posicionar el SGCN como ventaja competitiva.• Integrar resiliencia en estrategia comercial.
FA (Fortalezas + Amenazas)	• Usar backups robustos para mitigar ransomware. • Aprovechar liderazgo ejecutivo para responder ante crisis sísmica. • Activar protocolos ante cambios regulatorios.
DO (Debilidades + Oportunidades)	• Diversificar proveedores usando tecnología multi-cloud. • Formalizar simulacros periódicos. • Capacitación en continuidad aprovechando conciencia del mercado.
DA (Debilidades + Amenazas)	• Reducir dependencia tecnológica ante ciberataques. • Implementar plan de sucesión frente a crisis. • Asignar presupuesto para sitio alterno ante riesgo sísmico.

Partes interesadas y expectativas

Nº	Parte Interesada	Necesidades / Expectativas	¿Es obligación de cumplimiento? (Sí/No)	Requisito Aplicable	Relación con el SGCN
1	Clientes	Disponibilidad continua del servicio 24/7	Sí	SLA contractual	Define RTO y estrategias de continuidad
2	Regulador (SBS u otro)	Continuidad operativa y gestión formal de riesgos	Sí	Normativa regulatoria	Exige BIA, pruebas y planes documentados
3	Accionistas	Protección de ingresos y reputación	No (estratégico)	Gobierno corporativo	Justifica inversión en resiliencia
4	Empleados	Seguridad laboral y claridad de roles en crisis	Sí	Normativa laboral	Planes de comunicación y evacuación
5	Proveedores críticos	Cumplimiento de contratos y coordinación en contingencias	Sí	Contratos y SLA	Estrategia de gestión de terceros
6	Comunidad	Minimizar impacto social en caso de interrupción	No (expectativa social)	Responsabilidad social	Plan de comunicación de crisis

Alcance del SGCN

Declaración del alcance

- El Sistema de Gestión de Continuidad del Negocio (SGCN) de **la empresa** cubre los procesos, recursos y actividades necesarias para garantizar la continuidad de los servicios críticos ante eventos disruptivos que puedan afectar la operación.
- El SGCN aplica a:
  - Plataforma tecnológica principal y sistemas de soporte.
  - Procesos críticos identificados mediante el Análisis de Impacto al Negocio (BIA).
  - Infraestructura tecnológica, incluidos servidores, bases de datos y redes.
  - Personal clave involucrado en la operación de servicios críticos.
- Proveedores estratégicos cuya interrupción pueda afectar la continuidad.

Ubicación y Límites

- El alcance incluye:
  - Sede principal ubicada en Lima, Perú.
  - Infraestructura cloud utilizada para la prestación de servicios digitales.
  - Sitio alterno de recuperación ante desastres.
- Quedan excluidos del alcance:
  - Procesos administrativos no críticos.
  - Áreas comerciales que no afectan la prestación directa de servicios esenciales.

Riesgos presentes

- **Riesgo tecnológico:** Interrupción del servicio de pagos digitales debido a un ataque de ransomware que cifre los servidores productivos, generando indisponibilidad superior al RTO definido y pérdida de ingresos.
- **Riesgo de infraestructura:** Paralización de operaciones críticas causada por un corte eléctrico prolongado sin respaldo adecuado, afectando la continuidad del servicio y la atención al cliente.
- **Riesgo de proveedor:** Indisponibilidad de la plataforma tecnológica debido a la caída del proveedor cloud principal, impactando la prestación de servicios críticos y generando incumplimiento contractual.
- **Riesgo operacional:** Interrupción de procesos críticos por ausencia inesperada de personal clave sin plan de sucesión, afectando la capacidad de recuperación dentro del MTD establecido.
- **Riesgo natural:** Suspensión de operaciones en la sede principal a causa de un evento sísmico, provocando daños en infraestructura y retraso en la recuperación de los servicios esenciales.

3. Estructura de un plan de continuidad

Ejemplo de Política SGCN

- Se establece esta Política de Continuidad del Negocio como parte integral de su estrategia organizacional, con el propósito de asegurar la continuidad de sus productos y servicios críticos ante cualquier interrupción.
- La Alta Dirección se compromete a:
  - Proporcionar un marco para establecer y revisar los objetivos de continuidad del negocio.
  - Cumplir con los requisitos legales, regulatorios, contractuales y otros requisitos aplicables.
  - Proteger a las personas, activos, información y procesos esenciales.
  - Garantizar la disponibilidad de recursos necesarios para el funcionamiento eficaz del SGCN.
  - Mejorar continuamente la idoneidad, adecuación y eficacia del Sistema de Gestión de Continuidad del Negocio.
- Esta política es información documentada, será comunicada dentro de la organización y estará disponible para las partes interesadas pertinentes.

PIC Programa Integral de Capacitación en Gestión de Riesgos 2026

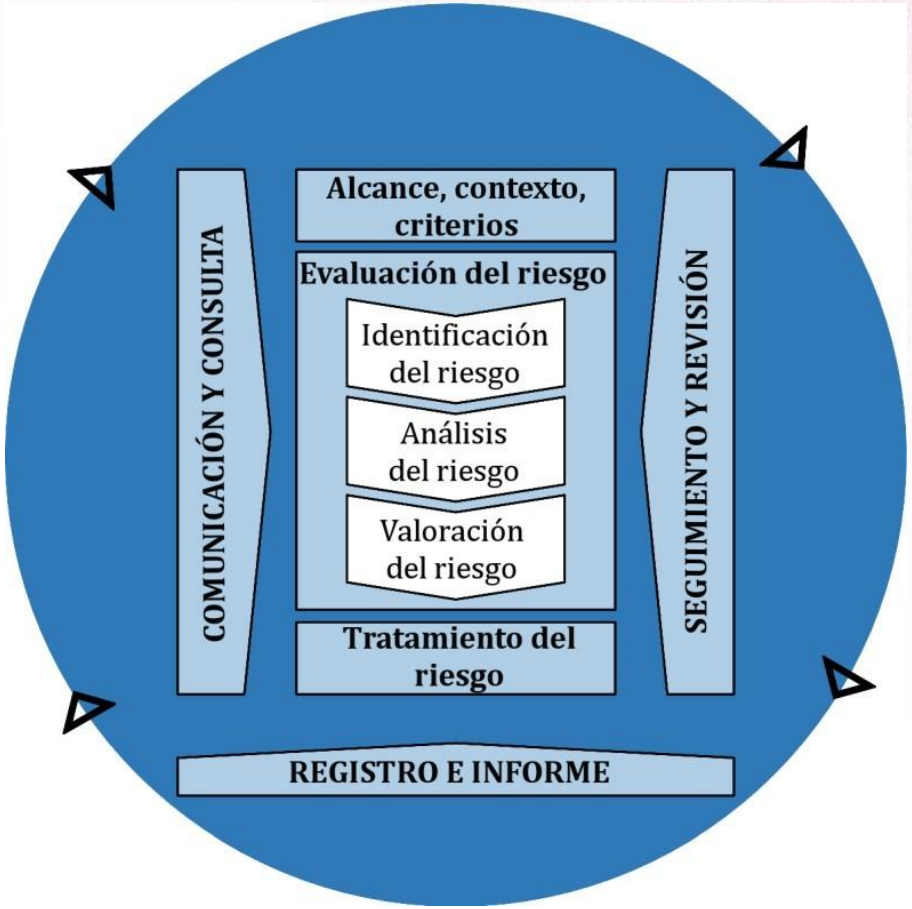
3.1 Gestión de riesgos de continuidad de negocios

RIMAC

fri·esan Finance & Regulation Institute

Gestión de riesgos

La gestión de riesgos es el proceso estructurado mediante el cual una organización identifica, analiza, evalúa y trata los riesgos que pueden afectar el logro de sus objetivos.



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

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.

Identificación, análisis y evaluación de riesgos

ID	Proceso Crítico	Amenaza	Evento de Riesgo	Impacto	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo (PxI)	Nivel
R1	Plataforma de pagos	Ransomware	Cifrado de servidores productivos	Interrupción total del servicio	4	5	20	Alto
R2	Core bancario	Caída de proveedor cloud	Indisponibilidad del servicio	Paralización de operaciones	3	5	15	Alto
R3	Atención al cliente	Ausencia de personal clave	Falta de operador crítico	Retraso en atención	3	3	9	Medio
R4	Infraestructura TI	Corte eléctrico prolongado	Falta de energía en sede principal	Interrupción operativa	2	4	8	Medio
R5	Base de datos financiera	Corrupción de datos	Pérdida parcial de información	Impacto financiero y reputacional	2	5	10	Medio

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.

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.

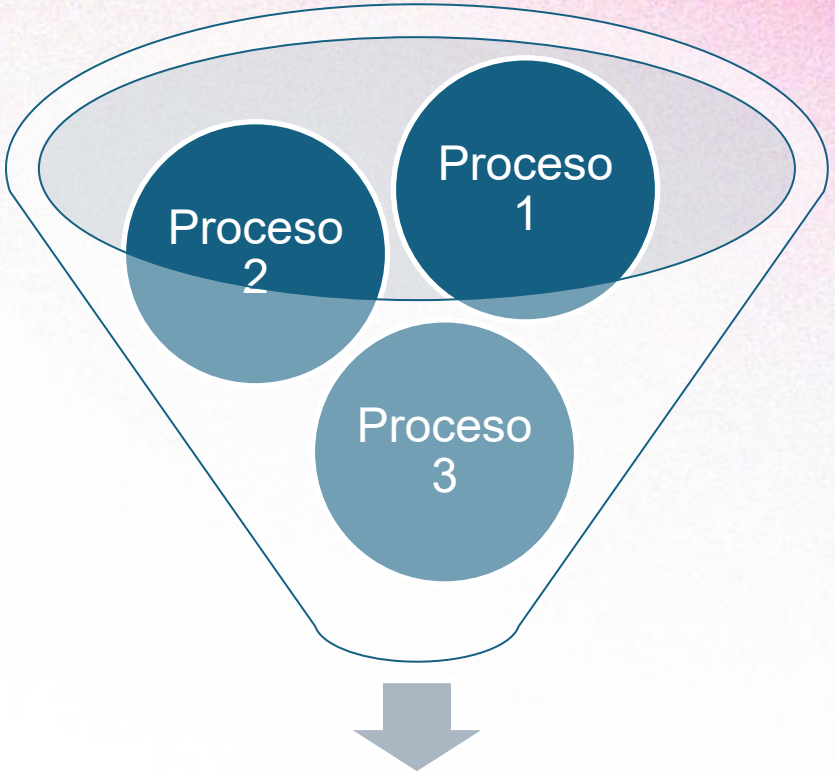
Tratamiento de riesgos

ID	Riesgo	Nivel	Estrategia de Tratamiento	Acciones Específicas	Responsable	Recursos Necesarios	Riesgo Residual
R1	Ransomware en plataforma de pagos	Alto	Reducir	Backups offline diarios, segmentación de red, EDR, pruebas de restauración trimestrales	CISO / TI	Infraestructura backup, licencias EDR	Medio
R2	Caída de proveedor cloud	Alto	Reducir / Transferir	Contrato multi-cloud, sitio alterno, SLA reforzado, pruebas de failover semestrales	CTO	Proveedor alterno, replicación	Medio
R3	Ausencia de personal clave	Medio	Reducir	Plan de sucesión, cross-training, manuales operativos documentados	RRHH / Operaciones	Plan capacitación	Bajo
R4	Corte eléctrico prolongado	Medio	Reducir	Generador de respaldo, mantenimiento UPS, prueba anual de autonomía	Operaciones	Generador, combustible	Bajo
R5	Corrupción de base de datos	Medio	Reducir	Replicación en tiempo real, monitoreo de integridad, backups incrementales	TI	Storage redundante	Bajo

3.2. Análisis de impacto al negocio

Análisis de Impacto al Negocio (BIA)

- Se usa para determinar los procesos críticos y los recursos relacionados en todas las unidades de negocio 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.
- 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.



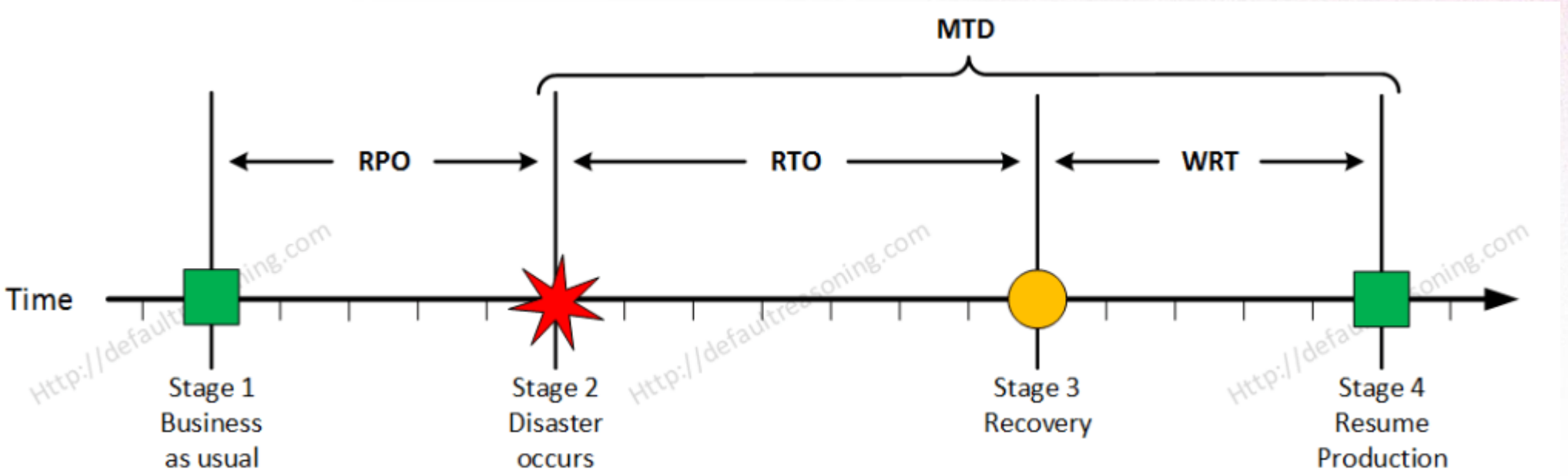
Análisis de Impacto al Negocio (BIA)

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.

Tiempos de recuperación



Análisis de impacto al negocio

ID	Proceso Crítico	Impacto Financiero	Impacto Operativo	Impacto Reputacional	Impacto Regulatorio	MTPD	RTO	RPO	Dependencias Clave	Nivel de Criticidad
B1	Plataforma de pagos	Muy Alto	Muy Alto	Alto	Alto	8 horas	4 horas	15 min	Core bancario, proveedor cloud, DB	Crítico
B2	Core bancario	Muy Alto	Muy Alto	Muy Alto	Alto	12 horas	6 horas	30 min	Data center, red, energía	Crítico
B3	Atención digital (web/app)	Alto	Alto	Alto	Medio	24 horas	8 horas	1 hora	Cloud, API pagos	Alto
B4	Gestión contable	Medio	Medio	Bajo	Alto	72 horas	48 horas	24 horas	ERP, base datos financiera	Medio
B5	RRHH / Nómina	Bajo	Medio	Bajo	Medio	5 días	72 horas	24 horas	Sistema planillas	Bajo

3.3. Estrategias de continuidad de negocio

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.

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.

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) 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.

Estrategias de continuidad de negocios.

ID	Proceso Crítico	Escenario de Interrupción	Estrategia de Continuidad	Tipo de Estrategia	RTO Objetivo	Recursos Requeridos	Responsable	Prueba Requerida
E1	Plataforma de pagos	Ransomware	Restauración desde backups offline + DR alterno	Recuperación TI	4 horas	Infraestructura DR, backup inmutable	CISO / TI	Prueba semestral
E2	Core bancario	Caída de data center	Activación de sitio alterno geográfico	Redundancia	6 horas	Data center alterno, replicación	CTO	Prueba anual
E3	Atención digital	Caída de proveedor cloud	Arquitectura multi-cloud	Diversificación	8 horas	Segundo proveedor cloud	TI	Failover trimestral
E4	Operación presencial	Sismo	Teletrabajo + activación de sede alterna	Alternativa operativa	24 horas	VPN, laptops, acuerdos coworking	Operaciones	Simulacro anual
E5	Personal clave	Ausencia prolongada	Plan de sucesión y cross-training	Organizacional	48 horas	Manuales, capacitación	RRHH	Revisión anual

Observaciones de Auditoría y Acciones Correctivas

ID	Tipo de Hallazgo	Requisito	Descripción del Hallazgo	Evidencia	Causa Raíz	Acción Correctiva	Responsable	Fecha Compromiso	Estado
A1	No Conformidad Mayor	8.2.2	No se realizó BIA formal para todos los procesos críticos	No existe matriz BIA actualizada	Falta de metodología definida	Elaborar y aprobar BIA completo	Gerente de Continuidad	30/04/2026	Abierto
A2	No Conformidad Menor	8.4	No se evidencian pruebas del BCP en el último año	No hay actas de simulacros	Falta de planificación anual	Programar y ejecutar simulacro anual	CISO	15/05/2026	En proceso
A3	Observación	5.2	Política de continuidad no menciona marco para objetivos	Política versión 1.0	Redacción incompleta	Actualizar política alineada a 5.2	Oficial de Cumplimiento	20/04/2026	Abierto
A4	Oportunidad de Mejora	7.2	Capacitación en continuidad no formalizada	No hay registro de capacitación	No existe plan formal	Implementar plan anual de capacitación	RRHH	30/06/2026	Pendiente
A5	No Conformidad Menor	9.2	Auditoría interna no cubrió todos los procesos del SGCN	Programa auditoría incompleto	Alcance mal definido	Actualizar programa de auditoría interna	Auditor Interno	10/05/2026	En proceso

3.4. Plan de Continuidad de Negocio (PCN)

Plan de continuidad

- **Objetivo**
  - Garantizar la continuidad de los servicios críticos ante interrupciones, asegurando recuperación dentro de los RTO definidos.
- **Procesos Críticos**
  - Plataforma principal de servicios digitales
  - Sistema financiero / ERP
  - Atención al cliente
  - Infraestructura tecnológica

Plan de continuidad

- **Tiempos Clave**
  - MTPD: 8 horas
  - RTO: 4 horas
  - RPO: 30 minutos
- **Escenarios de Activación**
  - Ataque ransomware
  - Caída de proveedor cloud
  - Corte eléctrico prolongado
  - Desastre natural

Plan de continuidad

- **Estrategias de Continuidad**
  - Backups offline e inmutables
  - Sitio alterno / infraestructura redundante
  - Teletrabajo para personal crítico
  - Contrato SLA con proveedores estratégicos

Plan de continuidad

- **Equipo de Crisis**
  - Director General (Líder)
  - CISO / TI (Recuperación tecnológica)
  - Operaciones (Continuidad operativa)
  - Comunicaciones (Gestión reputacional)
- **Comunicación**
  - Notificación interna inmediata
  - Comunicación a clientes
  - Reporte a regulador (si aplica)

Plan de continuidad

- **Pruebas y Mejora**
  - Simulacros anuales
  - Revisión semestral o anual del plan
  - Auditoría interna periódica

4. Ciclo de vida del PCN

Ciclo de vida del SGCN

PLAN				DO	CHECK	ACT
4. Contexto de la organización	5. Liderazgo	6. Planificación	7. Soporte	8. Operación	9. Evaluación	10. Mejora
Entendimiento de la organización y su contexto	Liderazgo y compromiso	Acciones de evaluación de riesgos y oportunidades	Recursos	Planificación operacional y control	Monitoreo, análisis y evaluación	No conformidad y acción correctiva
Entender las necesidades y expectativas de las partes interesadas	Política	Objetivos de continuidad de negocio	Competencias	Análisis de impacto al negocio y Evaluación del riesgo	Auditoria interna	Mejora continua
Determinar el alcance del SGCN	Roles y responsabilidades	Planificación de cambios del sistema de continuidad de negocio	Concientización	Plan de continuidad de negocio y procedimientos	Revisión de la gestión	
SGCN			Comunicación	Programa de ejercicios		
			Información documentada	Evaluación de la documentación de la continuidad del negocio y capacidades		

Conclusiones

- La continuidad del negocio es un elemento estratégico, no solo operativo.
- Las interrupciones son inevitables; la preparación marca la diferencia.
- El Análisis de Impacto al Negocio (BIA) permite identificar procesos críticos y definir RTO/RPO adecuados.
- La gestión de riesgos y las estrategias de continuidad reducen los impactos financieros, operativos y reputacionales.
- El compromiso de la Alta Dirección es fundamental para la eficacia del SGCN.
- Un sistema alineado con la ISO 22301 fortalece la resiliencia organizacional.
- Probar y mejorar continuamente el sistema garantiza la adaptación ante nuevos riesgos.
- La continuidad del negocio genera confianza, cumplimiento regulatorio y ventaja competitiva.

PIC

Programa Integral
de Capacitación

¡Gracias!

RIMAC

fri·esan
Finance & Regulation Institute