Continuidad de Negocio basada en la Generación de Valor

De la recuperación técnica a la resiliencia organizacional

Anticipar | Resistir | Responder | Recuperar | Adaptar

Fausto Mancheno, CBCP, COSO ERM

8vo Seminario Internacional de Riesgo Operativo

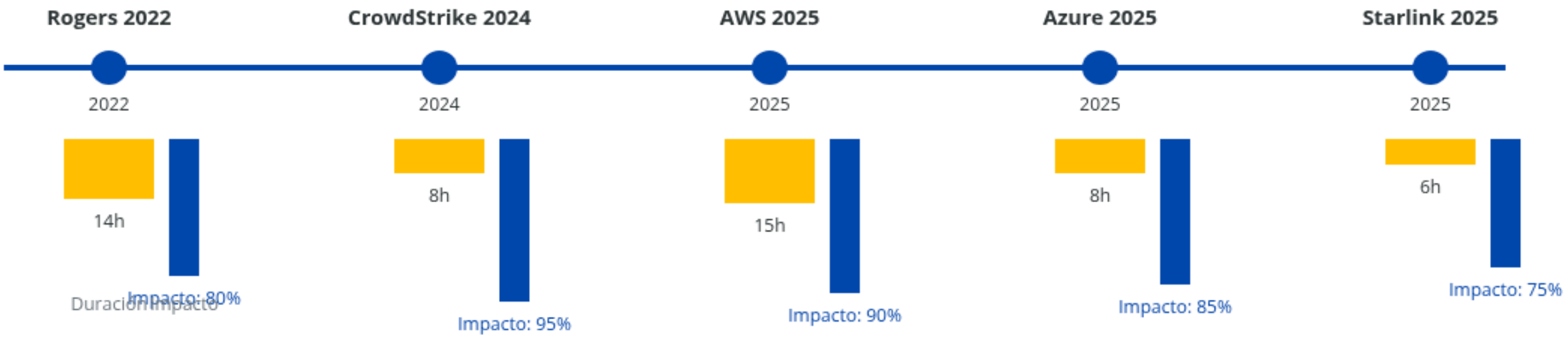
La Paradoja del Riesgo Moderno

La Paradoja del Riesgo Moderno

Rank 2024	Icon	Issue reference	Probability	Impact	Resilience index	Rank 2023	Rank +/–
1		Cyber Events	4.12	4.05	16.69	1	–
2		IT Disruption	3.76	3.76	14.14	2	–
3		Natural Disasters	3.34	3.25	10.86	4	Up 1
4		Financial Conditions	3.20	3.28	10.50	3	Down 1
5		HR Issues	3.18	2.99	9.51	5	–
6		Major Facility Incident	2.98	3.19	9.51	7	Up 1
7		Power Shortages	3.00	3.16	9.48	6	Down 1
8		Climate Change	3.24	2.90	9.40	9	Up 1
9		Increased Regulation	3.08	3.01	9.27	12	Up 3
10		Reputational Issues	2.91	3.13	9.11	11	Up 1

¿Qué pasa si un servicio crítico cae ocho horas?

En 2024, una simple actualización derribó millones de sistemas. En 2025, AWS y Azure demostraron que incluso la nube tiene su tormenta perfecta.



...La pregunta no es 'qué pasó', sino 'por qué no lo vimos venir'.

¿Qué pasa si un servicio crítico cae?

USD 5 400 M

Pérdida financiera directa estimada para las empresas Fortune 500 (excluida Microsoft) por la interrupción global del 19 de julio de 2024, originada en una actualización defectuosa de CrowdStrike Falcon. Estimación de Parametrix, julio de 2024.

- **USD 43,6 M**
  Pérdida media por empresa afectada afectada
- **1 de cada 4**
  Empresas Fortune 500 con interrupción interrupción de servicio
- **10 % – 20 %**
  Porción de la pérdida cubierta por seguro cibernético

Lo que la cifra no incluye

La estimación cubre pérdida directa de ingreso y margen. Quedan fuera la pérdida de productividad, el daño reputacional, la atrición de clientes y el costo de oportunidad de los equipos desviados a la respuesta. En la mayoría de los casos, ese remanente no medido supera a la pérdida directa reportada.

Su cifra, en 60 segundos

Impacto por hora =

(Ingreso operativo diario ÷ horas operativas) × % de dependencia del servicio
+ costo de recuperación por hora
+ penalidades contractuales y regulatorias por hora
+ costo de reprocesamiento manual

No sustituya este cálculo con referencias referencias de mercado: el directorio decide sobre su propia exposición, no no sobre la de terceros.

Fuente: Parametrix Insurance, «CrowdStrike's Impact on the Fortune 500» (2024). Cifras de pérdida directa, sin incluir daño reputacional ni pérdida de productividad. productividad.

¿Qué pasa si un servicio crítico cae?

Exposición a riesgos digitales en la región

Las organizaciones en LATAM enfrentan una combinación única de riesgos digitales amplificados por la fragilidad de su infraestructura:

Top 3 riesgos regionales: Ciberseguridad, cambio regulatorio y continuidad de negocio

Infraestructura frágil: Redes eléctricas y telecomunicaciones con menor redundancia

Alta dependencia: Concentración en pocos proveedores cloud y fintech

Evolución regulatoria: Tendencia hacia modelos tipo DORA

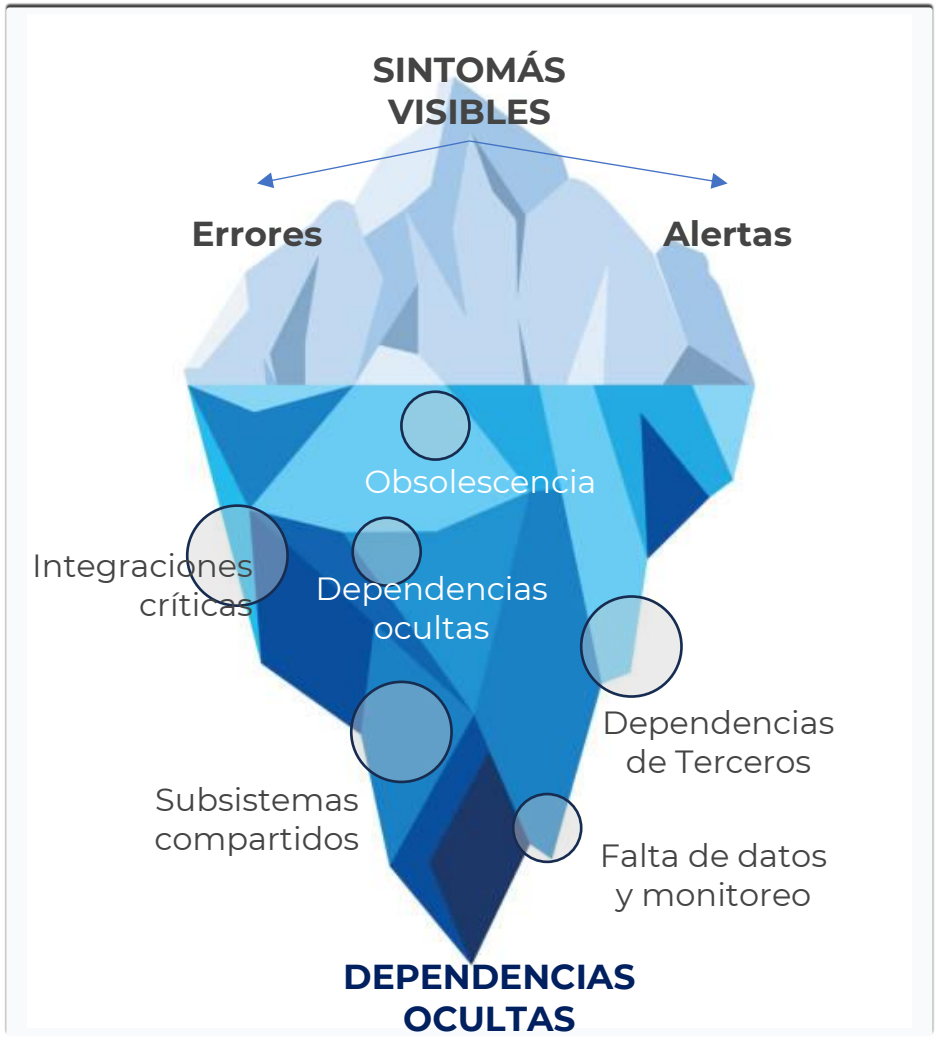
Fuente: Análisis compuesto de IIA LATAM Risk in Focus 2025 y BCI Horizon Scan Report

Panaroma Global

¿Porqué fallamos?:
La raíz de las disrupciones modernas

- Dependencias ocultas y concentración de riesgo en subsistemas compartidos (DNS, health checks, etc.)
- Falta de telemetría y observabilidad end-to-end
- Cambios no controlados y despliegues sin capacidad de rollback
- Modelos estáticos de resiliencia desconectados de datos en tiempo real
- Falta de datos para anticipar degradación temprana

Mensaje clave:
"El enemigo no es el evento... es la ceguera operativa."



La continuidad de negocio debe debe evolucionar de «recuperar «recuperar sistemas» a «preservar «preservar y generar valor» mediante resiliencia organizacional.

1. **Anticipar**
   Inteligencia y preparación
2. **Resistir**
   Arquitectura y redundancia
3. **Responder**
   Equipos y comunicación
4. **Recuperar**
   Restitución del servicio
5. **Adaptar**
   Aprendizaje obligatorio

El cambio no es semántico. Redefine el objeto de gestión (el valor entregado, no el activo técnico), el titular técnico), el titular de la decisión (la línea de negocio, no la mesa de servicio) y el criterio de éxito (continuidad (continuidad del servicio al cliente, no restauración del componente).

Por qué fallan los programas de continuidad

1

Enfoque técnico y en silos

El plan cubre servidores; no cubre decisiones, clientes ni proveedores. Continuidad se delega a TI y el negocio no reconoce autoría.

2

Planes vigentes, capacidad inexistente

Documento actualizado y aprobado, nunca ejercitado. La vigencia formal se confunde con capacidad real de ejecución.

3

Métricas desconectadas del negocio

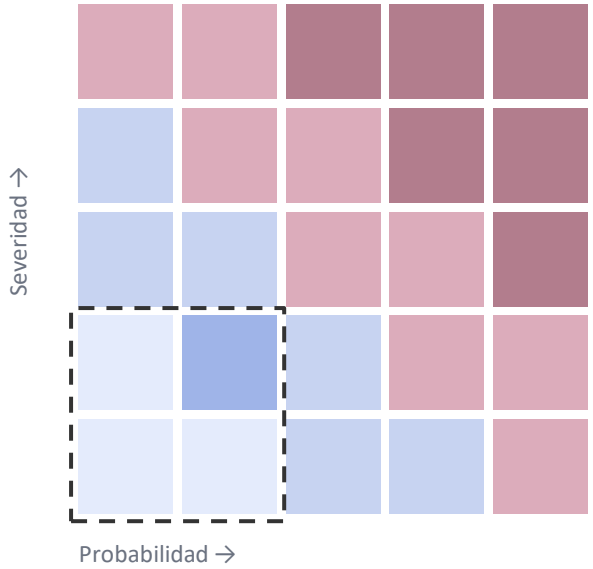
RTO expresado en horas técnicas sin traducción traducción a pérdida de valor. El comité no no puede priorizar lo que no puede comparar. comparar.

4

Cadena de proveedores no resiliente

Se hereda el RTO del eslabón más débil. El El certificado del proveedor sustituye a la prueba conjunta.

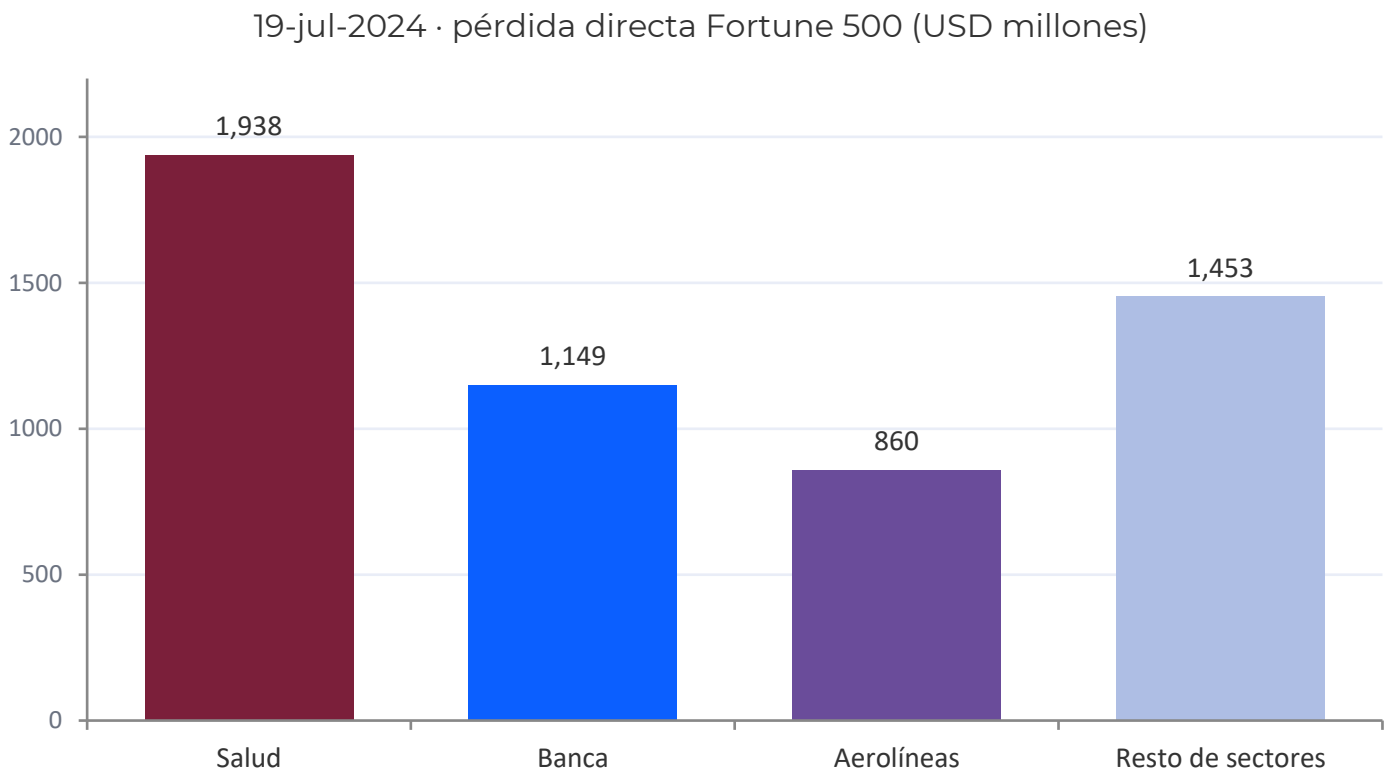
Dónde se concentra el esfuerzo



El programa típico invierte donde hay evidencia evidencia histórica abundante (recuadro): eventos eventos frecuentes y de baja severidad. La pérdida pérdida material se concentra en el vértice opuesto, opuesto, donde no hay serie histórica y sí hay exposición.

Mapa ilustrativo del sesgo de asignación de esfuerzo; no representa datos de una entidad concreta.

Dónde se concentró la pérdida



57 % de la pérdida

Salud y banca concentraron el 57 % del total pese a representar el 20 % de los ingresos del listado. La exposición no es proporcional al tamaño.

Impacto no financiero

El reporte BCI 2025 documenta efectos simultáneos sobre desempeño operativo, experiencia del cliente y salud mental del personal.

Transferencia limitada

El seguro cibernético absorbió entre el 10 % y el 20 %. La La retención efectiva del riesgo permanece en el balance. balance.

Fuentes: Parametrix Insurance (2024) para las cifras por sector; el valor «Resto de sectores» es residual calculado sobre el total de USD 5 400 M. BCI Horizon Scan Report 2025 para los impactos no financieros.

De la recuperación técnica a la resiliencia

Enfoque tradicional

- RTO y RPO como objetivo final del programa
- Respaldo, replicación y sitio alterno
- Alcance acotado a la infraestructura de TI
- Prueba anual de recuperación, en ventana controlada
- Éxito = el sistema fue restaurado

Enfoque de resiliencia

- Continuidad del valor entregado al cliente
- Degradación controlada diseñada por servicio
- Alcance extremo a extremo, incluidos terceros
- Programa de ejercicios multinivel y no anunciados
- Éxito = el servicio y la confianza se sostuvieron

Lo que no cambia

El RTO y el RPO no se abandonan: se subordinan.

Siguen siendo el instrumento de ingeniería, pero dejan de ser el objetivo de gestión. Se fijan desde el impacto en el valor y no desde la capacidad instalada de la plataforma.

Un RTO fijado por lo que la infraestructura puede dar es una descripción; fijado por lo que el negocio tolera es un requisito.

Encuadre conceptual construido sobre ISO 22301:2019 (cláusula 8) y BCI Good Practice Guidelines, edición 7.0 (2023).

Integración de la Resiliencia al Modelo Operativo

Antes del Desastre | Durante el Desastre | Después del Desastre

Gestión de Riesgos

Prevención de interrupciones en los negocios mediante identificación y tratamiento

Preparación

- Ambiente y contexto
- Comunicación y consulta

Evaluación

- Identificación
- Análisis
- Evaluación

Acción

- Tratamiento del riesgo
- Seguimiento continuo

Resiliencia Operacional

Resistencia a los riesgos e interrupciones

Continuidad del Negocio

Recuperación y mantenimiento de funciones críticas

Respuesta de Emergencia

- Plan de crisis y comités
- Equipos de respuesta
- Evacuaciones y protocolos

Gestión de Crisis

- Comunicación y comando
- Centros de mando móviles
- Decisiones estratégicas

Continuidad y Recuperación

- Planes de continuidad de TI
- Estrategias de BCP y DRP

Resiliencia organizacional: definición operativa

Capacidad de una organización para absorber el impacto de una disrupción, adaptarse a un entorno entorno cambiante y continuar entregando valor a clientes y partes interesadas dentro de umbrales umbrales acordados.

1

Anticipación

Detectar la señal antes antes del evento

2

Resistencia

Absorber sin colapsar la la entrega

3

Respuesta

Decidir y comunicar bajo bajo presión

4

Recuperación

Restituir el servicio priorizado

5

Adaptación

Cambiar la organización organización tras el evento

Relevancia para el directorio: la resiliencia es el único atributo que convierte un riesgo no evitable en un riesgo gobernado. No gobernado. No reduce la probabilidad del evento; reduce la varianza del resultado.

Formulación operativa construida a partir de la familia ISO 22300 / ISO 22301:2019 y de BCI GPG 7.0. No constituye cita textual de la norma; verifique el texto normativo vigente en iso.org antes de citarla como definición formal.

Marcos y estándares vigentes

ISO 22301:2019

Requisitos certificables del sistema de gestión de de continuidad. Enmienda 1:2024 sobre acción climática. Una nueva edición está en desarrollo (ISO/CD (ISO/CD 22301, en revisión de comité).

Familia ISO complementaria

ISO 22313 (directrices de implantación), ISO/TS 22317 (análisis de impacto al negocio), ISO 22318 (continuidad de la cadena de suministro), ISO 22361 (gestión de crisis).

BCI GPG, edición 7.0

Publicada en 2023 bajo modelo de documento vivo. Seis prácticas profesionales: dos de gestión y cuatro técnicas. Reemplaza el «ciclo de vida» por «sistema de gestión».

DRI Professional Practices

Diez prácticas profesionales, revisadas en 2023-2024. 2024. Base del cuerpo de conocimiento y de la certificación CBCP. Disponibles en varios idiomas. idiomas.

COSO ERM 2017

«Integrating with Strategy and Performance». Cinco componentes y veinte principios. Vincula la gestión de riesgos con la estrategia y el desempeño, no con el control.

DORA — Reg. (UE) 2022/2554

Aplicable desde el 17 de enero de 2025. Cinco pilares: riesgo TIC, reporte de incidentes, pruebas de resiliencia, riesgo de terceros TIC e intercambio de información.

Fuentes: iso.org (ISO 22301:2019 y ISO/CD 22301), thebci.org (GPG 7.0), drii.org (Professional Practices), coso.org (ERM 2017), eur-lex.europa.eu (DORA). Confirme la edición vigente de cada norma ISO complementaria norma ISO complementaria antes de citarla en documentación formal.

MARCOS Y TEORÍA · 8 MIN

Lo que todos los marcos exigen

1	**Analizar el impacto y priorizar** Determinar qué procesos sostienen la entrega de valor y en qué plazo su interrupción se vuelve se vuelve material.	ISO 22301 § 8.2	DRI PP 3
2	**Evaluar el riesgo de disrupción** Identificar amenazas sobre los recursos que soportan las actividades priorizadas y tratar la tratar la exposición.	ISO 22301 § 8.2	DRI PP 2
3	**Definir estrategias y soluciones** Decidir cómo se sostendrá cada actividad priorizada dentro de su plazo, con recursos comprometidos.	ISO 22301 § 8.3	DRI PP 4
4	**Estructurar respuesta y planes** Definir activación, roles, procedimientos y comunicación antes del evento, no durante.	ISO 22301 § 8.4	DRI PP 5–6
5	**Ejercitar, evaluar y mejorar** Validar la capacidad mediante un programa de ejercicios y cerrar hallazgos con responsable y responsable y plazo.	ISO 22301 § 8.5–8.6	DRI PP 8

Las prácticas técnicas de BCI GPG 7.0 cubren la misma secuencia; la numeración de sus prácticas se omite aquí por no haber sido verificada contra el texto de la edición vigente.

Correspondencia elaborada por el ponente sobre ISO 22301:2019 (cláusula 8) y DRI Professional Practices. Verifique la numeración de cláusulas contra el texto normativo antes de usarla como evidencia de auditoría. como evidencia de auditoría.

Qué hacen distinto las organizaciones líderes

1

Simulaciones ejecutivas

El comité de dirección ejercita la decisión, no solo la aprueba. War games con información incompleta y presión de tiempo real.

2

Integración estructural

Continuidad, ciberseguridad y cadena de suministro comparten análisis de impacto, escenarios y calendario de pruebas.

3

Métricas de impacto

Los indicadores se expresan en pérdida pérdida evitada y servicio sostenido, no sostenido, no en porcentaje de planes planes actualizados.

4

Cultura de decisión

Se entrena decidir con información parcial y se protege al que decide. La La ausencia de decisión es el modo de de falla más caro.

El indicador silencioso de madurez: quién vigila el horizonte

El BCI Horizon Scan 2025 midió cómo se realiza el análisis de tendencias. La cifra relevante no es la mayoría, sino el residuo: una de cada cinco organizaciones no ejecuta análisis de tendencias en absoluto y, por tanto, planifica su continuidad exclusivamente sobre eventos ya ocurridos.

47,9 %
Función corporativa central

23,5 %
Enfoque descentralizado descentralizado

21,1 %
No lo ejecuta

Fuente: BCI Horizon Scan Report 2025 (publicado el 19 de noviembre de 2025), thebci.org. Los porcentajes no suman 100 % por respuestas restantes no detalladas en la nota de prensa.

Tres mitos que frenan la resiliencia

«Con un sitio alterno basta»

Realidad

El sitio alterno resuelve infraestructura. No resuelve resuelve quién autoriza la activación, cómo se se informa al cliente, ni qué hace el proceso mientras el sistema vuelve. La interrupción del 19- del 19-jul-2024 no se resolvía conmutando de de centro de datos: los dispositivos de usuario final usuario final requerían intervención manual.

«La seguridad lo cubre todo»

Realidad

Ciberseguridad gestiona la probabilidad; continuidad gestiona la consecuencia. DORA las trata como pilares diferenciados dentro de un mismo reglamento, precisamente porque una no sustituye a la otra. El evento de 2024 no fue un ataque y aun así detuvo la operación global.

«No hay presupuesto para esto»

Realidad

El costo de la interrupción ya está en el estado de estado de resultados: aparece como pérdida operativa, reproceso, sobretiempo y atrición de de clientes. La decisión no es gastar o no gastar, sino gastar, sino si el gasto será presupuestado y gobernado o incurrido y no atribuido.

Fuentes de apoyo: Reglamento (UE) 2022/2554 (DORA), estructura de pilares; Parametrix Insurance (2024) sobre la naturaleza no adversarial del evento de julio de 2024.

¿Documento o capacidad?

Plan

Un artefacto documental. Se redacta, se aprueba, se versiona y se se audita. Su existencia se demuestra mostrando el archivo. Su estado estado por defecto es «vigente».

Capacidad

Un comportamiento repetible bajo presión. Se entrena, se mide y se mide y se degrada si no se usa. Su existencia solo se demuestra demuestra ejecutándola. Su estado por defecto es «no verificada». verificada».

La aritmética de la capacidad

Capacidad = Plan × Personas entrenadas × Decisión ejercitada × Recursos comprometidos

Es un producto, no una suma. Si cualquier factor vale cero, el resultado es cero, por muy alto que sea el valor de los demás. Un plan excelente multiplicado por cero personas entrenadas sigue siendo cero.

Implicación de gestión: el indicador que importa no es el porcentaje de porcentaje de planes actualizados, sino el porcentaje de planes ejecutados al menos una vez de principio a fin por las personas que que deberán ejecutarlos.

Encuadre conceptual del ponente, alineado con el requisito de programa de ejercicios de ISO 22301:2019 § 8.5 y con el pilar de pruebas de resiliencia operativa digital de DORA.

El nuevo paradigma de la resiliencia

Modelo de madurez 1.0 → 4.0

1.0 Documental

Planes estáticos, enfoque de cumplimiento, documentación manual

2.0 Adaptativa

Escenarios probados, análisis de impacto, simulacros periódicos

3.0 Predictiva

Métricas en tiempo real, dashboards vivos, detección temprana

4.0 Autónoma

IA + automatización, runbooks inteligentes, optimización continua

Basado en modelos de madurez de continuidad de negocios DRI/BCI

El nuevo paradigma de la resiliencia

Capacidades críticas y ruta de mejora recomendada

Existen 4 capacidades críticas para la resiliencia operacional:

1. Monitoreo continuo

Visibilidad en tiempo real del estado operativo

2. Modelos avanzados

Analytics predictivos para identificar patrones

3. Evaluación de terceros

Monitoreo de proveedores con telemetría

4. Gestión de datos e IA

Automatización de respuestas y decisiones

Visión 2026:

Transformar la continuidad: de respuesta reactiva a identificación proactiva y mitigación automática.

Basado en: DRI International Resilience Framework 2024-2025

Framework: cinco capacidades esenciales

1 **Anticipar**
Análisis de impacto vivo, vigilancia de amenazas y mapa de dependencias dependencias de terceros.

2 **Resistir**
Degradación controlada por diseño, redundancia selectiva y acuerdos de acuerdos de servicio exigibles.

3 **Responder**
Estructura de activación, roles decididos antes del evento y comunicación comunicación preaprobada.

4 **Recuperar**
Restitución priorizada por valor, con objetivos derivados del impacto y no impacto y no de la plataforma.

5 **Adaptar**
Revisión post-incidente con acciones obligatorias y cambio efectivo de efectivo de proceso o arquitectura.

Anticipar: inteligencia y preparación

1

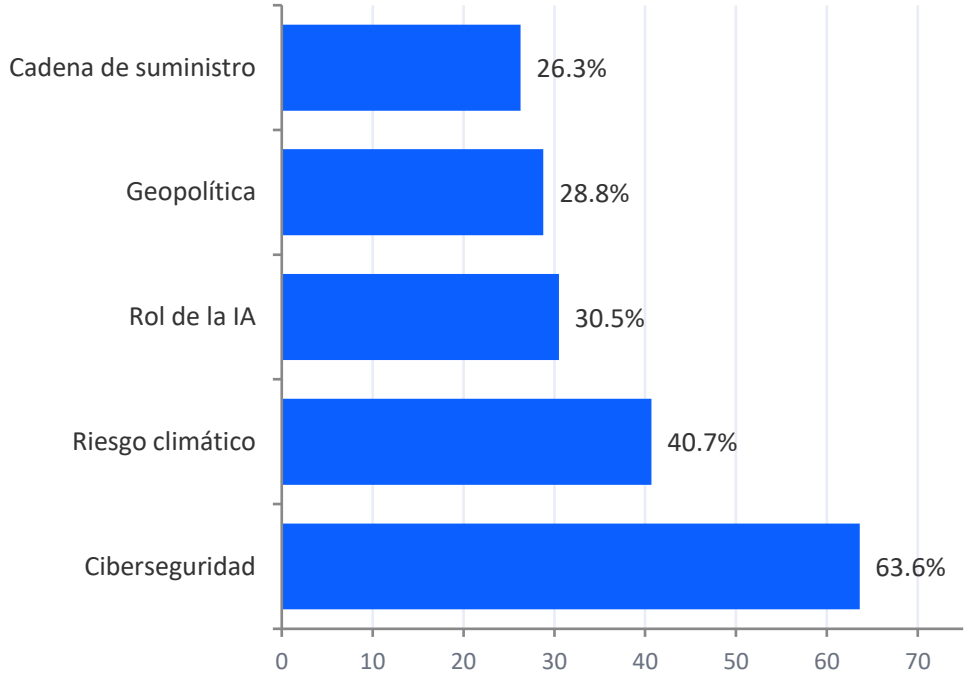
- Análisis de impacto vivo: se revisa ante todo cambio material de de proceso, no por calendario anual.
- Vigilancia de amenazas conectada a la operación, con dueño designado y frecuencia definida.
- Inventario de proveedores críticos con el objetivo de recuperación heredado hecho explícito.

Prácticas concretas

Fije disparadores de revisión del análisis de impacto —no solo periodicidad—; incorpore la incorpore la vigilancia de amenazas como punto fijo del comité de continuidad; declare el continuidad; declare el objetivo de recuperación heredado de cada proveedor crítico proveedor crítico junto al objetivo propio, para que la brecha sea visible.

Señal de madurez: el análisis de impacto modificó al menos una decisión de inversión en los últimos doce meses.

Principales preocupaciones a 5–10 años (% de profesionales)



Fuente: BCI Horizon Scan Report 2025, thebci.org. Encuesta a profesionales de continuidad y resiliencia; los porcentajes reflejan selección múltiple y no suman 100 %.

Anticipar: inteligencia y preparación

Identificación anticipada de riesgos mediante análisis multidimensional...

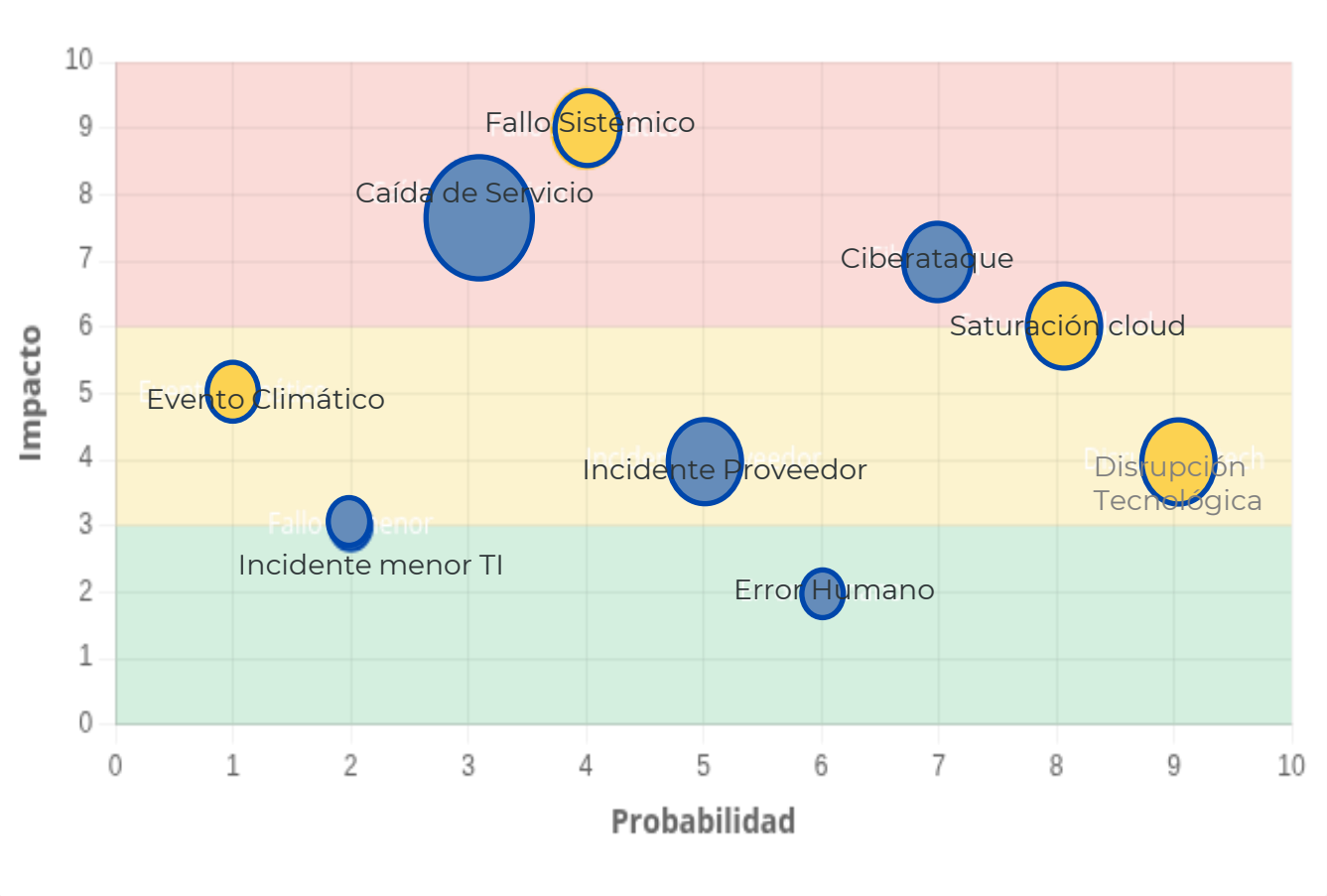
Modelos predictivos aplicados:

ARIMA / SARIMA
Series temporales para tendencias

Análisis de Drift
Detección de cambios graduales

Redes Bayesianas
Análisis probabilístico de dependencias

AIOps / ML
Detección avanzada de anomalías



Matriz de riesgos por nivel de impacto:

- Bajo (monitoreo estándar)
- Medio (alertas ampliadas)
- Alto (intervención inmediata)

- Riesgos actuales
- Riesgos emergentes

CAPACIDAD 2 DE 5 · RESISTIR

Resistir: arquitectura y redundancia

2

- Degradación controlada diseñada por servicio: definir qué se deja de hacer, no solo hacer, no solo qué se sostiene.
- Redundancia selectiva, dimensionada por criticidad. Duplicar todo es tan ineficiente como no duplicar nada.
- Acuerdos de nivel de servicio exigibles con proveedores críticos, con derecho contractual de prueba conjunta.

Prácticas concretas

Documente el modo degradado de cada servicio crítico con su umbral de activación y su límite de límite de duración; revise los acuerdos de nivel de servicio anualmente y en cada renovación renovación contractual; incorpore el derecho de auditoría y de prueba conjunta como cláusula, no como cláusula, no como cortesía.

Señal de madurez: existe al menos un servicio crítico que ya operó en modo degradado de forma planificada, no planificada, no forzada por un incidente.

Diseño por niveles de continuidad

Nivel 1

Alta disponibilidad activa. Sin pérdida perceptible de servicio. servicio.

Nivel 2

Modo degradado documentado, con capacidad reducida y anunciada.

Nivel 3

Reanudación diferida con procedimiento manual acotado en el tiempo.

El costo crece con el nivel; la cobertura debe seguir al valor, no al organigrama.

Encuadre de diseño del ponente; alineado con ISO 22301:2019 § 8.3 (estrategias y soluciones de continuidad) e ISO 22318 (continuidad de la cadena de suministro).

CAPACIDAD 2 DE 5 · RESISTIR

Resistir: arquitectura y redundancia

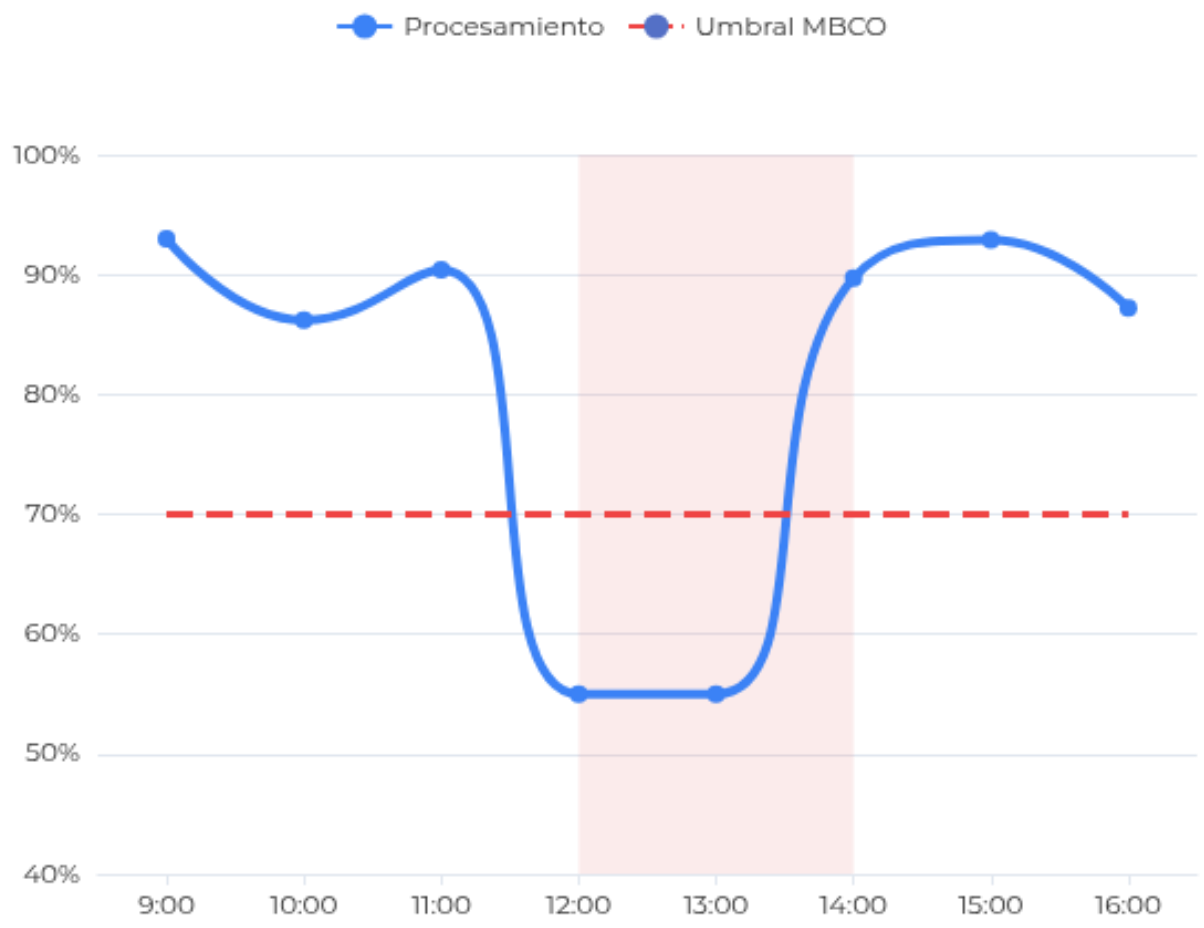
MBCO Dinámico: Anticipación operativa con métricas en vivo

Contexto: Procesamiento de transacciones bancarias

Demanda normal: 10.000 transacciones/hora

MBCO establecido: 70% de capacidad

Evento detectado: Degradación al 55%



Criterio de alerta:

La caída por debajo del umbral durante 30+ minutos activa alerta antes que los clientes perciban problemas.

Acciones recomendadas:

- ✓ **Escalamiento técnico inmediato**
- ✓ **Runbooks de contención**
- ✓ **Monitoreo de backlog en tiempo real**

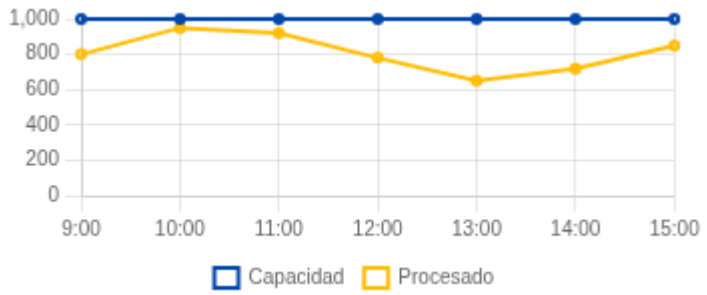
Resistir: arquitectura y redundancia

Monitoreo en tiempo real de métricas críticas para anticipar interrupciones antes de que impacten al cliente.

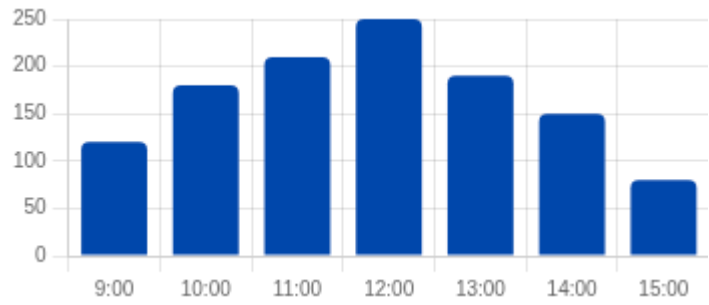
Acciones derivadas:

- Activar DRP si múltiples indicadores en rojo
- Convocar comité de crisis ante primer indicador
- Comunicación preventiva a stakeholders clave

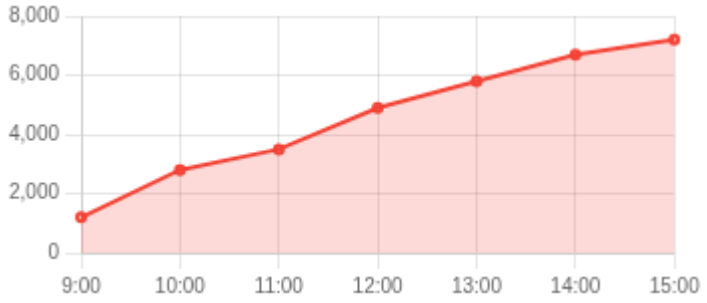
Capacidad vs Procesado



Backlog Horario



Backlog Acumulado



Riesgo de Crisis

CAPACIDAD 3 DE 5 · RESPONDER

Responder: equipos, decisión y comunicación

3

- Roles y matriz de responsabilidad decididos antes del evento, con con suplencia designada y verificada.
- Manuales de actuación de una página, accionables por servicio, no manuales extensos por sistema.
- Comunicación interna y externa preaprobada por Legal y Cumplimiento antes de la crisis.

Prácticas concretas

Designe un único responsable de activación por escenario, con autoridad explícita autoridad explícita para decidir con información incompleta; mantenga plantillas plantillas de comunicación revisadas y versionadas; ensaye el primer mensaje, mensaje, que es el que fija la narrativa de todo el evento.

Señal de madurez: cualquier miembro del equipo de respuesta puede nombrar, sin consultar, quién consultar, quién activa y a quién se informa primero.

Ventanas de decisión

1 **0 – 15 min**
Detectar, declarar y designar. No se diagnostica: se se declara.

2 **15 – 60 min**
Activar modo degradado, informar a partes internas y al regulador si aplica.

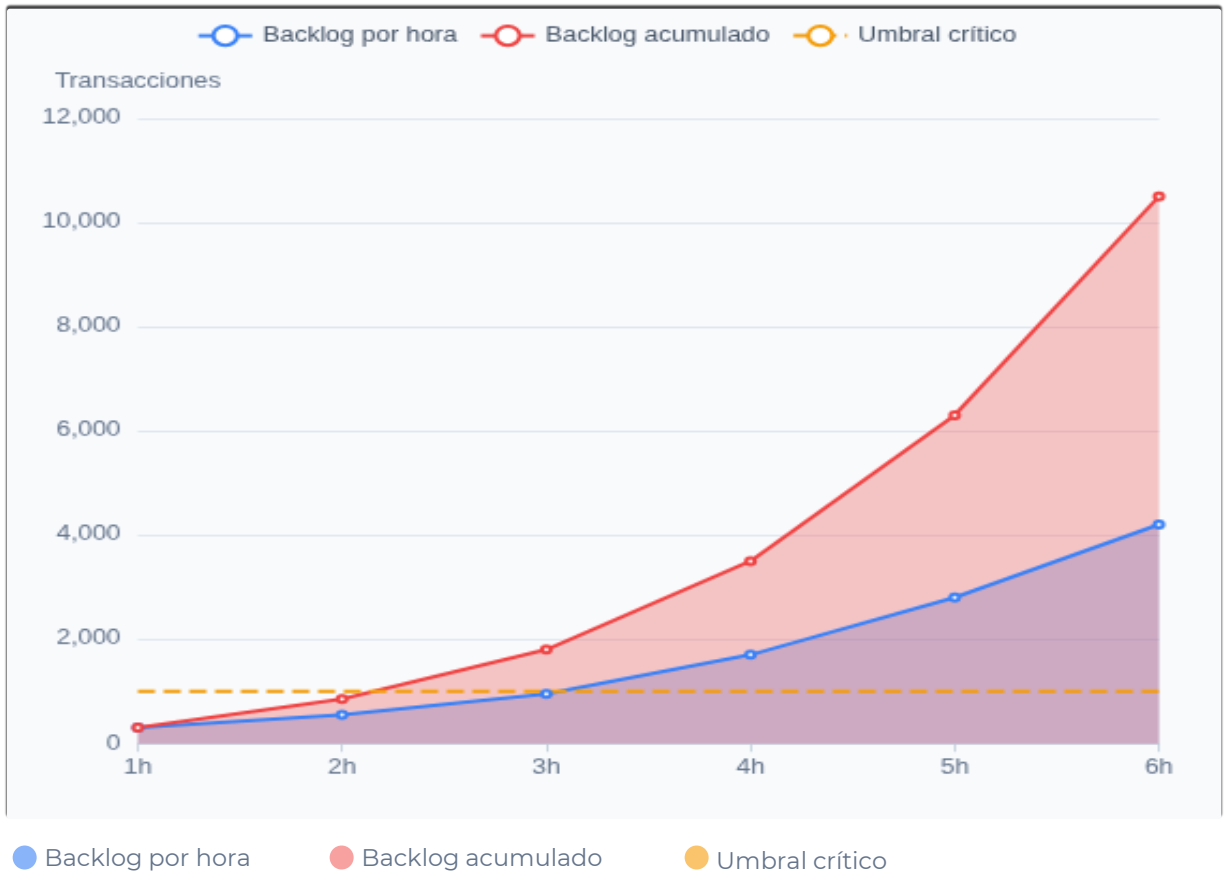
3 **60 – 240 min**
Estabilizar, comunicar externamente y sostener el ciclo el ciclo de actualización.

4 **> 240 min**
Relevo de turnos, gestión de fatiga y preparación del preparación del cierre del evento.

Estructura de ventanas propuesta por el ponente sobre ISO 22301:2019 § 8.4 (estructura de respuesta, alerta y comunicación) e ISO 22361 (gestión de crisis).

Responder: equipos, decisión y comunicación

MBCO Dinámico: Backlog y crecimiento exponencial del riesgo



Riesgo crítico:

87% probabilidad de indisponibilidad total del servicio en la próxima hora, con tiempo estimado de recuperación >12 horas.

Decisiones recomendadas:

1. Activar failover regional hacia datacenter alternativo
2. Implementar priorización de colas críticas (pagos, autorizaciones)
3. Activar control dinámico de tráfico y comunicación a clientes

CAPACIDADES 4 Y 5 · RECUPERAR Y ADAPTAR

Recuperar y adaptar: volver, y volver distinto

4 Recuperar

- Objetivos de recuperación derivados del impacto impacto real, no de la capacidad instalada.
- Restitución priorizada por valor entregado, con secuencia acordada previamente.
- Verificación de integridad antes de declarar el servicio restablecido.

5 Adaptar

- Revisión post-incidente con acciones obligatorias, obligatorias, responsable y plazo.
- Cambio efectivo en arquitectura o proceso como salida exigida de la lección.
- Reingreso del aprendizaje al análisis de impacto y a la vigilancia de amenazas.

Regla de las 72 horas

La revisión post-incidente se realiza dentro de dentro de las 72 horas siguientes al cierre, cierre, mientras la memoria operativa está está intacta.

Cada hallazgo sale con responsable y fecha. Riesgos audita el cierre.

Una revisión sin acciones cerradas no es aprendizaje: es documentación del fracaso.

Caso de referencia — A.P. Møller-Maersk, NotPetya (junio de 2017): reinstalación de aproximadamente 4 000 servidores, 45 000 equipos y 2 500 aplicaciones en diez días, con un aplicaciones en diez días, con un impacto estimado por la propia compañía entre USD 250 y 300 millones. La organización operó manualmente durante la recuperación. La lección recuperación. La lección declarada por su presidente fue de adaptación, no de recuperación: convertir la ciberseguridad en ventaja competitiva.

Fuente: declaraciones de Jim Hagemann Snabe, presidente de A.P. Møller-Maersk, en el Foro Económico Mundial (Davos, enero de 2018), recogidas por medios especializados. Cifra de impacto estimada por la compañía. impacto estimada por la compañía.

Recuperar y adaptar: volver, y volver distinto

Métricas clave de resiliencia:

RTO (Recovery Time Objective)

Tiempo máximo tolerable de recuperación medido y auditado en pruebas periódicas.

Backlog

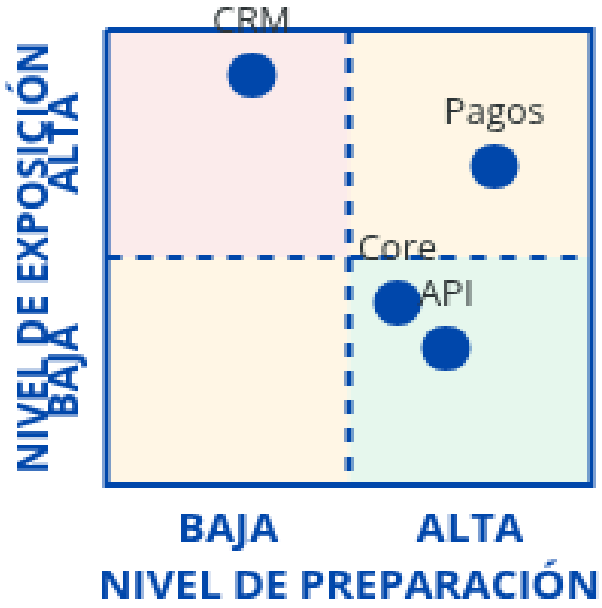
Acumulación de transacciones pendientes con umbrales claros de activación de contingencia.

Runbooks

Procedimientos operativos estandarizados con cobertura medida de escenarios críticos.

Deuda de resiliencia

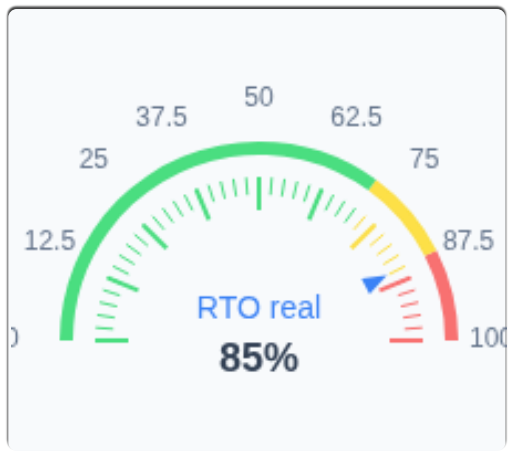
Cuantificación de vulnerabilidades conocidas y no remediadas con plan de reducción.

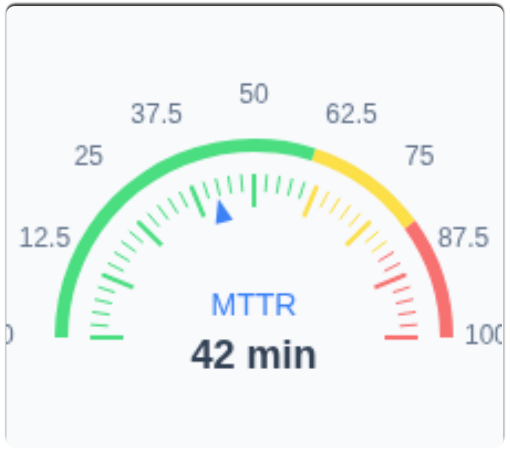


CAPACIDADES 4 Y 5 · RECUPERAR Y ADAPTAR

Recuperar y adaptar: volver, y volver distinto

Métricas clave para decisiones basada en datos





Basado en framework de métricas de resiliencia operativa DRI/BCI

Beneficio estratégico:

Las métricas de resiliencia permiten priorizar inversiones, validar controles y construir confianza con stakeholders a través de datos objetivos.

Hoja de ruta 0–6 meses: arranque

1

Ejecutar el análisis de impacto al negocio

Inventario de servicios con impacto cuantificado, objetivo de recuperación derivado del negocio y negocio y dependencias declaradas.

Responsable

Riesgos y dueños de proceso

Mes 1–2

2

Clasificar proveedores y revisar acuerdos

Clasificación por criticidad, objetivo de recuperación heredado y brecha contractual documentada. documentada.

Responsable

Riesgos, Legal y Compras

Mes 2–3

3

Construir tres manuales de actuación

Manuales de una página por servicio, con activación, roles, ventanas de decisión y mensajes base. mensajes base.

Responsable

Continuidad y dueños de servicio

Mes 3–4

4

Fijar indicadores y ejercitar un escenario

Línea base de objetivo de recuperación real, tiempo medio de restitución y disponibilidad, más disponibilidad, más informe de ejercicio con hallazgos.

Responsable

Continuidad y Tecnología

Mes 5–6

Criterio de salida de la fase: existe un análisis de impacto aprobado, tres manuales ejecutables y un ejercicio realizado con hallazgos asignados. Sin esos cuatro elementos, la fase no está cerrada fase no está cerrada aunque el cronograma se haya cumplido.

Secuencia propuesta por el ponente sobre ISO 22301:2019 (cláusula 8) y BCI GPG 7.0. Los plazos son indicativos y deben ajustarse al tamaño y complejidad de cada organización.

Hoja de ruta 6–18 meses: maduración

1

Mes 6–9

Integrar continuidad, ciberseguridad y riesgo de terceros

Análisis de impacto, escenarios y calendario de pruebas compartidos entre las tres las tres funciones, con gobierno único.

2

Mes 6–18

Instaurar un programa de ejercicios y simulaciones

Ejercicio de mesa trimestral, simulación técnica semestral y ejercicio ejecutivo anual, ejecutivo anual, con hallazgos auditados.

3

Mes 9–15

Automatizar y orquestar la recuperación de servicios críticos

Procedimientos de conmutación ejecutables y verificados, con reducción medible del tiempo de restitución.

4

Mes 12–18

Medir el impacto financiero evitado y reportarlo al directorio

Método documentado de estimación, línea base comparable y reporte periódico al órgano de gobierno.

Regla de reporte al directorio: un indicador de exposición, un indicador de capacidad y un indicador de aprendizaje. Tres cifras, una página, cadencia fija. Más de tres indicadores en el órgano indicadores en el órgano de gobierno se convierten en información sin decisión asociada.

Secuencia propuesta por el ponente. Las frecuencias de ejercicio son recomendación profesional; ISO 22301:2019 § 8.5 exige un programa de ejercicios sin fijar periodicidad, y DORA establece obligaciones de prueba para establece obligaciones de prueba para las entidades bajo su ámbito.

Convergencia: continuidad, ciber y tecnología

Continuidad

Prioriza servicios por valor y define umbrales de tolerancia. tolerancia.

Ciberseguridad

Reduce probabilidad, detecta y contiene el evento adversarial.

Tecnología

Sostiene la arquitectura, la redundancia y la restitución técnica.

Base común obligatoria: un único análisis de impacto · un catálogo de servicios compartido · un calendario de pruebas conjunto · una taxonomía de incidentes única

- Sin catálogo de servicios común, cada función prioriza un universo distinto y las las prioridades se contradicen en el evento.
- Sin taxonomía única de incidentes, el reporte al órgano de gobierno no es consolidable y la exposición agregada queda invisible.
- Sin ejercicios conjuntos, las dependencias ocultas entre funciones solo se descubren en producción y bajo presión.

El precedente regulatorio: DORA

Reglamento (UE) 2022/2554, aplicable desde el 17 de enero de 2025. Estructura la resiliencia operativa digital en cinco pilares obligatorios:

1. Gestión del riesgo de TIC
2. Gestión y reporte de incidentes de TIC
3. Pruebas de resiliencia operativa digital
4. Gestión del riesgo de terceros de TIC
5. Intercambio de información

Aunque su ámbito jurídico es la Unión Europea, define un un estándar de referencia para entidades con contrapartes o contrapartes o proveedores bajo ese perímetro.

Fuente: Reglamento (UE) 2022/2554 (DORA), eur-lex.europa.eu. Aplicable desde el 17 de enero de 2025.

Proveedores: el eslabón que fija su objetivo real

- Clasifique por criticidad de servicio, no por volumen de gasto. El proveedor más barato más barato puede sostener el proceso más crítico.
- Pruebe la continuidad con el proveedor. El certificado acredita un sistema de gestión; no acredita que la conmutación funcione con usted.
- Documente el objetivo de recuperación heredado junto al propio. Su objetivo real es el mayor de los dos, no el que usted declaró.
- Defina estrategia de salida y alternativa validada antes de la dependencia, no durante la interrupción.

La aritmética que se omite

Si su objetivo de recuperación declarado es de 4 horas y su proveedor crítico sostiene 24 horas sin 24 horas sin compromiso contractual de prueba conjunta, su objetivo real es de 24 horas. La horas. La diferencia no es una brecha técnica: es una declaración inexacta ante el órgano de órgano de gobierno y ante el supervisor.

Contexto de riesgo 2026

El Global Risks Report 2026 del Foro Económico Mundial sitúa la confrontación geoeconómica como principal riesgo del año, señalada por el 18 % de los encuestados como el más probable para desencadenar una crisis global, y advierte sobre su efecto en las cadenas de suministro.

En paralelo, el BCI Horizon Scan 2025 ubica el fallo de terceros y de infraestructura crítica entre las cinco principales preocupaciones a doce meses, junto a ciberataques, clima extremo, interrupciones de TI y telecomunicaciones, y filtraciones de datos.

Marco aplicable: ISO 22318 y el cuarto pilar de DORA.

Fuentes: World Economic Forum, The Global Risks Report 2026 (14 de enero de 2026); BCI Horizon Scan Report 2025 (19 de noviembre de 2025).

Indicadores que el órgano de gobierno puede usar

Indicador	Definición operativa	Fuente del dato	Dimensión
Cumplimiento del objetivo de recuperación	Servicios críticos cuyo tiempo real de restitución se mantuvo dentro del objetivo declarado	Ejercicios e incidentes reales	Capacidad
Tiempo medio de restitución	Promedio de restitución del servicio priorizado, con tendencia tendencia trimestral	Registro de incidentes	Capacidad
Disponibilidad de servicios críticos	Cumplimiento del umbral acordado con el negocio, por servicio y no agregado	Monitoreo de servicio	Exposición
Impacto financiero evitado	Pérdida estimada que no se materializó, con método de cálculo documentado	Modelo propio auditable	Exposición
Cierre de acciones post-incidente	Hallazgos cerrados dentro del plazo comprometido sobre el total generado	Revisiones post-incidente	Aprendizaje

Los valores meta se fijan sobre la propia línea base. No importe referencias de mercado como objetivo: una meta que la organización no puede explicar es una meta que no defenderá en auditoría. defenderá en auditoría.

Conjunto propuesto por el ponente, alineado con ISO 22301:2019 § 9.1 (seguimiento, medición, análisis y evaluación) y con la lógica de vinculación entre riesgo y desempeño de COSO ERM 2017.

Practicar para no improvisar

1 Ejercicio de mesa

Discusión guiada sobre escenario, sin ejecución técnica. Entrena decisión, roles y comunicación.

Recomendado: trimestral

2 Simulación técnica

Ejecución real de conmutación y restitución sobre entorno controlado. Valida procedimientos.

Recomendado: semestral

3 Ejercicio ejecutivo

Escenario con información incompleta y presión de tiempo para el comité de dirección.

Recomendado: anual

Diseño de un ejercicio de cuatro horas

0:00 encuadre y reglas · 0:20 inyección inicial y primera decisión · 1:00 inyección de agravamiento con con información contradictoria · 2:00 comunicación externa simulada · 2:45 inyección de recuperación parcial · recuperación parcial · 3:15 cierre del escenario · 3:30 evaluación en caliente con los participantes · 4:00 4:00 asignación de hallazgos con responsable y fecha

El error más común

Diseñar el ejercicio para que salga bien. Un ejercicio que no que no produce hallazgos no midió capacidad: midió midió familiaridad con el guion. El indicador de un buen buen ejercicio es el número de acciones correctivas que que genera.

Frecuencias indicadas como recomendación profesional del ponente. ISO 22301:2019 § 8.5 exige un programa de ejercicios y evaluación sin fijar periodicidad; DORA establece obligaciones específicas de prueba para las específicas de prueba para las entidades bajo su ámbito.

Cómo construir el caso de inversión

Método de estimación de exposición evitada

Exposición anual esperada = impacto por hora × duración esperada del evento × frecuencia anual
frecuencia anual estimada

Beneficio del programa = exposición sin gestión − exposición con gestión − costo anual del programa

Los cuatro parámetros que debe obtener antes de la reunión

1	**Impacto por hora**	Finanzas y dueño de proceso	Ingreso operativo, reproceso, penalidades
2	**Duración esperada**	Continuidad y Tecnología	Tiempo real observado en incidentes y ejercicios
3	**Frecuencia anual**	Riesgos	Registro histórico propio más análisis de tendencias
4	**Costo del programa**	Continuidad	Personas, plataforma, ejercicios y auditoría

Cómo presentarlo al directorio

- Abra con el costo de no hacer nada, no con el costo el costo del programa.
- Exprese la exposición en la moneda y el horizonte que el directorio ya usa para decidir.
- Presente un rango con sus supuestos explícitos, nunca una cifra puntual sin intervalo.
- Muestre qué decisión concreta se solicita y qué ocurre si se difiere un año.
- Comprometa la métrica de seguimiento en la misma lámina en que pide el presupuesto.

Método propuesto por el ponente. Los parámetros deben obtenerse de fuentes internas verificables; no se recomienda usar promedios de mercado como sustituto de la línea base propia.

Empiece hoy: tres pasos concretos

30 días

Ejecute un análisis de impacto acotado

Sobre los tres servicios de mayor valor. No busque cobertura total: busque discriminación válida entre lo crítico y lo importante.

60 días

Construya tres manuales y ejercite uno

Una página por servicio. El ejercicio debe producir hallazgos; si no los produce, el diseño falló.

90 días

Reporte tres indicadores al comité

Uno de exposición, uno de capacidad y uno de uno de aprendizaje. Comprometa la cadencia cadencia en la misma sesión.

La resiliencia deja de ser un costo de cumplimiento el día en que la organización puede demostrar, con evidencia propia, qué valor propia, qué valor sostuvo mientras otros lo perdían.

¡Muchas Gracias!

Tres preguntas frecuentes

1. ¿Cómo empezar con presupuesto limitado?
2. ¿Cómo integrar continuidad con ciberseguridad?
3. ¿Cómo medir el impacto financiero evitado?

Fausto Mancheno
CBCP Certified | ISO 31000, 22301, 37001 | COSO ERM