Guía para la **Gestión de Riesgo** de CiberSeguridad

No todas las decisiones de riesgo fallan por falta de información.
Muchas fallan por algo más difícil de ver.

Las organizaciones saben qué riesgos enfrentan,
qué está en juego
y cuentan con marcos, controles y capacidades para gestionarlos.

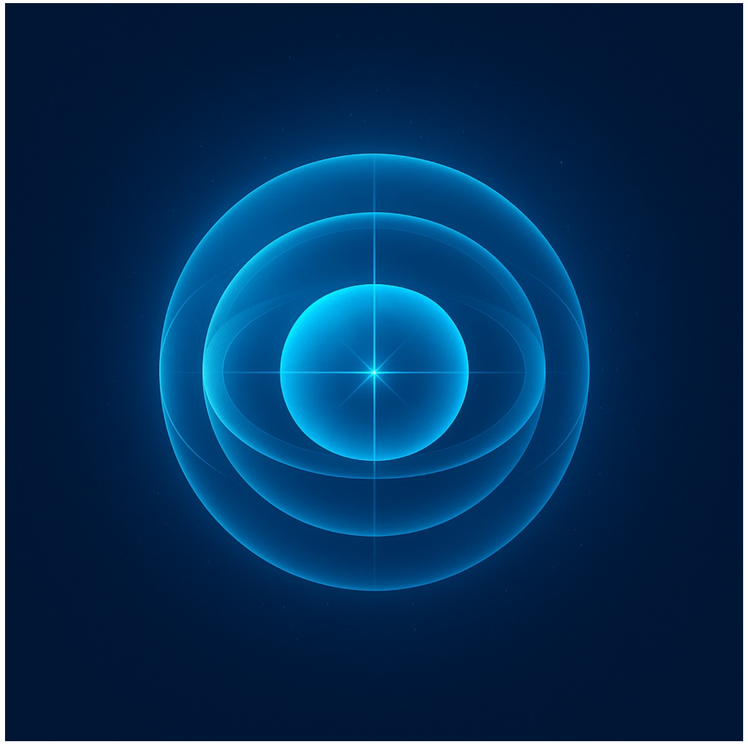
Aun así, las decisiones no siempre son coherentes.

Esto no ocurre en cada decisión por separado,
sino en cómo se conectan entre sí.

Esta guía comienza por observar cómo se decide frente a la incertidumbre.

A partir de ahí, presenta un enfoque que integra la comprensión del entorno, la capacidad de respuesta y la acción efectiva.

No como un ciclo,
sino como una estructura viva que evoluciona con la organización.



LUIS ALEJANDRO PEREZ

Estructura **Viva**

A partir de esta forma de observar el riesgo, la gestión deja de ser un conjunto de controles y se convierte en una estructura que evoluciona con la organización.

Este enfoque que integra la madurez humana,
la gestión tecnológica
y la generación de valor.

Más que un modelo, es una forma de pensar el riesgo como una estructura viva, capaz de aprender, adaptarse y demostrar resultados.

Se expresa como un sistema compuesto por tres capas interdependientes que evolucionan en equilibrio permanente:

- Su exterior representa la **conciencia** — la visión y comprensión amplia del entorno y de la exposición organizacional.
- Su cuerpo intermedio encarna la **capacidad** — la acción sistémica que equilibra control, aprendizaje y evolución.
- Su núcleo irradia la **acción** efectiva — la resiliencia medible que traduce el esfuerzo en evidencia y valor tangible.

Visión Integradora

A partir de esta base, la gestión del riesgo se traduce en decisiones concretas con tres propósitos:

- **Fortalecer la capacidad de decidir**
  Evaluar la coherencia entre conciencia, capacidad y acción frente a la incertidumbre. Define el nivel de madurez desde el que la organización decide ante el riesgo.

- **Gobernar con coherencia**
  Evaluar la robustez del gobierno y la gestión del riesgo tecnológico y operacional. Alinea la práctica con los marcos de referencia internacionales.

- **Generar valor sostenible**
  Medir el retorno operativo y económico de la resiliencia. Integra escenarios y costos permitiendo justificar la inversión en continuidad.

Así, la gestión del riesgo dirige la incertidumbre con propósito.

El riesgo no se elimina,
se transforma.

Convergencia Estratégica

Etapa	Anticipar Impacto →	Proteger Valor →	Justificar Retorno →	Evolucionar Madurez
	 Determinar **Situación del Riesgo**	 Determinar **Escenarios y Eventos**	 Determinar **Inversión Sustentable**	 Determinar **Plan de Gestión**

Actividades	• **Exposición Humana**
	  • Coherencia del desempeño
	• **Exposición Tecnológica**
	  • Gobierno
	  • Gestión
	  • Infraestructura
	• Indicador
	  • **Indice de Riesgo Real**
		• **Análisis de escenarios:** tecnológicos, operacionales y humanos.
		• **Estimación de impacto** alineado al negocio.
		• **Priorización** en términos monetarios y de continuidad.
		• **Definición de niveles de riesgo:** aceptación y límites de tolerancia.
			• Calcular **Valor Económico Total Evitado.**
			• Determinar **Costo Total de Propiedad** de la estrategia actual.
			• Identificar **Margen de Tolerancia** según nivel de madurez.
			• Establecer **Inversión Mínima Sustentable**.
				• **Mitigación priorizada**
				• **Programa de Sensibilización y Cultura**

Instrumento	• Modelo de Evaluación de Gobierno y Gestión de Riesgo Operacional Tecnológico • Indice Compuesto de Madurez Digital • Indice de Riesgo Real	• Métricas financieras y operativas de continuidad	• Indice Compuesto de Valor en Continuidad • Métricas financieras y operativas de Continuidad	• InfoSeg Empática • Programa de Sensibilización CyberVida • Programa de Capacitación CyberDefensa

Los instrumentos mencionados forman parte de una línea metodológica en evolución, integrada por los modelos ICMD, G2ROT e ICVC. Cada uno representa una dimensión práctica de la gestión del riesgo como estructura viva, actualmente en desarrollo y mejora continua.

Estructura viva. Riesgo coherente. Valor medible.

Determinar **Situación del Riesgo**

Propósito

Identificar el nivel real de exposición de la organización frente a amenazas tecnológicas y humanas, evaluando tanto la madurez de su gestión como la coherencia del desempeño individual y colectivo.

Esta etapa permite establecer una línea base objetiva que refleje el riesgo real, no solo el percibido, y define el punto de partida para todas las decisiones posteriores.

Instrumentos

- **Modelo G2ROT**: Evalúa la madurez del gobierno, la gestión y la infraestructura tecnológica en materia de riesgo operacional y ciberseguridad.
- **Índice Compuesto de Madurez Digital (ICMD)**: Determina la coherencia entre conciencia, capacidad y acción frente al riesgo.
- **Índice de Riesgo Real (IRR)**: Integra ambas dimensiones y refleja la exposición global de la organización.

Metodologia

1. Evaluar la exposición tecnológica (G2ROT)
- Analizar el gobierno: políticas, roles, estructura de decisión y trazabilidad.
- Evaluar la gestión: efectividad operativa, monitoreo y respuesta ante incidentes.
- Examinar la infraestructura: capacidades, dependencias, obsolescencia y resiliencia técnica.

2. Evaluar la exposición humana (ICMD)
- Analizar la coherencia entre conciencia, capacidad y acción.
- Identificar brechas de madurez decisional y cultura de riesgo.
- Evaluar la postura organizacional ante la incertidumbre.

3. Integrar resultados y calcular el Índice de Riesgo Real (IRR)
- Combinar los resultados ponderados de G2ROT e ICMD.
- Asignar pesos relativos según criticidad y nivel de madurez organizacional.
- Generar una puntuación global de exposición al riesgo.

4. Validar la coherencia global
- Revisar que los resultados reflejen la realidad operativa y cultural.
- Corregir sobrestimaciones o subestimaciones mediante revisión de contexto.

Indicadores y Resultados

El resultado de esta etapa es un Índice de Riesgo Real (IRR) entre 0 y 1, que expresa el nivel de exposición total.

Rango IRR	Interpretación	Acción
≥0,80	Riesgo Controlado	Mantener y revisar periódicamente los controles.
0,50 - 0,79	Riesgo Moderado	Fortalecer áreas de debilidad y mejorar cultura organizacional.
<0,50	Riesgo Alto	Priorizar mitigaciones y definir planes urgentes de acción.

El IRR puede desagregarse por área o dominio, permitiendo analizar tanto la vulnerabilidad tecnológica como la madurez humana.

Los resultados del IRR sirven como entrada principal para la Etapa 2, permitiendo enfocar el análisis en los escenarios de riesgo crítico más probables y con mayor impacto.

De esta forma, la evaluación inicial asegura que los recursos se asignen a los riesgos reales y no a percepciones subjetivas.

Determinar **Escenarios y Eventos**

Propósito

Identificar, clasificar y priorizar los escenarios y eventos de riesgo que podrían generar un impacto económico, operativo o reputacional significativo.

Esta etapa transforma los resultados de exposición (IRR) en información accionable, permitiendo enfocar la gestión en lo verdaderamente crítico para el negocio.

Instrumentos

- **Resultados del IRR (Etapa 1):** Base de exposición tecnológica y humana.
- **Métricas Financieras y Operativas de Continuidad (ICVC):** Determinan el impacto económico esperado de cada evento.
- **Matriz de Escenarios Críticos (MEC):** Relaciona exposición, impacto y prioridad.
- **Modelos de BIA y de probabilidad ajustada:** Complementan el análisis contextual.

Metodologia

1. Identificar escenarios potenciales

- Revisar el contexto operativo, normativo y de mercado.
- Mapear eventos pasados, vulnerabilidades y amenazas emergentes.
- Incorporar escenarios provenientes de auditorías, incidentes y análisis BIA.

2. Analizar impacto y probabilidad

- Estimar el impacto financiero y operativo de cada escenario.
- Asignar niveles de probabilidad en función de madurez, controles y entorno.
- Traducir ambos factores a un valor económico estimado.

3. Priorizar riesgos críticos

- Cruzar los resultados del IRR (exposición) con los valores de impacto.
- Definir la matriz de riesgo ajustada a la realidad del negocio.
- Clasificar los riesgos como aceptables, moderados o no aceptables.

4. Definir límites de aceptación y tolerancia

- Establecer criterios de decisión según la capacidad de absorción de pérdidas.
- Documentar los umbrales de riesgo máximo aceptable (RMA).
- Integrar los resultados al proceso de decisión estratégica.

Indicadores y Resultados

El producto de esta etapa es una Matriz de Escenarios Críticos, que clasifica los riesgos según su criticidad económica y operacional.

Nivel de Riesgo	Descripción	Criterio de Acción
Crítico $R \geq 0.8$	Escenarios con alto impacto y alta probabilidad.	Requieren mitigación inmediata o transferencia del riesgo.
Moderado $0{,}50 \leq R < 0{,}80$	Impacto o probabilidad media.	Requieren seguimiento y planes de mitigación progresiva.
$R < 0{,}50$	Impacto limitado y baja probabilidad.	Riesgos aceptables, con control básico y monitoreo periódico.

Cada escenario se describe con su impacto económico estimado (USD) y su nivel de continuidad afectado (procesos, servicios, reputación, etc.).

Los escenarios críticos priorizados se convierten en insumos para la Etapa 3, donde se evalúa el costo-beneficio de invertir en mitigaciones, controles o estrategias de continuidad.

De esta forma, el proceso asegura que la inversión se base en datos tangibles y no en percepciones o modas de riesgo.

Determinar **Inversión Sustentable**

Propósito

Establecer el nivel óptimo de inversión en continuidad y mitigación del riesgo, garantizando equilibrio entre valor protegido, costos operativos y retorno económico.

Esta etapa demuestra que la resiliencia no es un gasto, sino una inversión estratégica sustentable, capaz de justificar cada acción con base en evidencia cuantificable.

Instrumentos

- **ICVC (Índice Compuesto de Valor en Continuidad):** modelo base para cuantificar valor, costos y retorno.
- **Métricas Financieras y Operativas:** extraídas de los escenarios críticos (Etapa 2).
- **Tablas de Margen de Tolerancia (T):** ajustan el análisis según nivel de madurez.
- **Proyección de Inversión Mínima Sustentable (IMS):** evalúa viabilidad y retorno.

Metodologia

1. Calcular el Valor Económico Total Evitado (VETE)
- Identificar los beneficios financieros derivados de la continuidad: ingresos protegidos, productividad recuperada, costos evitados, multas no incurridas, retención de clientes.
- Cuantificar el valor total preservado por las medidas de continuidad ante cada escenario crítico.

2. Determinar el Costo Total de Propiedad (TCO)
- Incluir todos los costos asociados a la estrategia de continuidad: implementación, capacitación, mantenimiento, infraestructura, pruebas y simulacros.
- Diferenciar entre costos fijos y variables, y proyectar su comportamiento en el tiempo.

3. Establecer el Margen de Tolerancia (T)
- Aplicar un margen proporcional según el nivel de madurez de la organización:
  Básico→ T=10% | Intermedio→ T=7% | Avanzado→ T=5%

4. Calcular la Inversión Mínima Sustentable (IMS)
- Aplicar la relación: IMS = (VETE+T)/TCO
- Interpretar los resultados según el equilibrio entre costo y valor.

5. Validar con la Dirección Financiera y Operativa
- Contrastar resultados con presupuestos y proyecciones.
- Ajustar inversiones priorizando las que maximizan retorno o reducen exposición crítica.

Indicadores y Resultados

El producto final es la Inversión Mínima Sustentable (IMS), que define el punto donde la inversión en continuidad protege valor sin sobredimensionar costos.

Resultado	Interpretación	Acción Recomendada
IMS ≥ 1	Inversión justificada.	Mantener y optimizar el plan de continuidad.
0.8 ≤ IMS <1	Inversión parcialmente sustentable.	Revisar asignación de recursos y eficacia de los controles.
IMS < 0,50	Inversión no sustentable.	Reevaluar costos, beneficios o alcance de la estrategia.

Los resultados financieros obtenidos aquí son la base de la Etapa 4: Determinar Plan de Gestión, que organiza las acciones según prioridad, costo y retorno.

Así, la toma de decisiones se alinea tanto con la estrategia financiera como con la continuidad operativa y cultural.

Determinar
Plan de Gestión

		Metodologia	Indicadores y Resultados
Propósito	Traducir los resultados del análisis y la inversión sustentable en acciones concretas, cultura organizacional y mejora continua.	**1. Definir medidas de mitigación** • Priorizar según el Nivel de Madurez del Gobierno y la Gestión de Riesgos. • Clasificar cada medida por criticidad y por impacto financiero y operacional. • Documentar responsables, plazos y métricas de éxito, asegurando criterios de cumplimiento. **2. Diseñar estrategias de sensibilización** • Identificar públicos clave y adecuar mensajes al nivel de madurez digital de cada grupo. • Integrar la sensibilización en las rutinas organizacionales. • Medir el impacto cultural con indicadores de coherencia y participación. **3. Establecer programas de fortalecimiento:** • Diseñar rutas de formación por perfil, combinando formación técnica y capacitación en criterio y responsabilidad digital. • Programar simulacros y pruebas periódicas de respuesta y recuperación para evaluar efectividad operativa. • Certificar competencias o avances de madurez tras cada ciclo de formación. **4. Integrar el seguimiento:** • Definir indicadores de avance y resultado alineados a los objetivos de resiliencia. • Establecer frecuencia para analizar desvíos y ajustes. • Realimentar las etapas anteriores del modelo.	Establecer indicadores que midan y evidencien el progreso y madurez de la organización en aspectos como por ejemplo: Eficacia Operativa y Coherencia Cultural **Indicador** / **Qué mide** / **Qué demuestra** Mitigaciones dentro del plazo proyectado — Cumplimiento del plan de mitigación en tiempo y alcance. — Eficiencia operativa y capacidad de ejecución de la gestión de riesgos. % Medidas con cumplimiento verificado — Relación de acciones implementadas con evidencia validada — Madurez del control y trazabilidad del proceso (reflejo del gobierno efectivo). % Participación en programa de sensibilización — Tasa de adhesión del personal a actividades de sensibilización. — Nivel de compromiso organizacional con la cultura de continuidad y seguridad. Índice de coherencia cultural — Relación entre conciencia, capacidad y acción post-programa. — Evolución del comportamiento organizacional frente al riesgo.
Instrumentos	• **InfoSeg Empática** → sensibilización desde la empatía y la conciencia digital. • **Programa CyberVida** → cultura digital y responsabilidad cotidiana. • **Programa CyberDefensa** → formación técnica y estratégica de largo plazo.		Cierra el ciclo, transformando decisiones en acciones medibles. Los resultados obtenidos alimentan nuevamente la evaluación de exposición y madurez (Etapa 1), fortaleciendo el proceso de mejora continua.

Resiliencia Medible

Evaluar → *Integrar* → *Relacionar* → *Demostrar*

La resiliencia no es un estado.
Es una práctica que se demuestra en cómo se decide.

Medirla implica traducir
el esfuerzo en valor,
el control en retorno
y la continuidad en confianza.

Cuando esto se hace desde un criterio compartido,
las decisiones se vuelven consistentes
y el valor se sostiene.

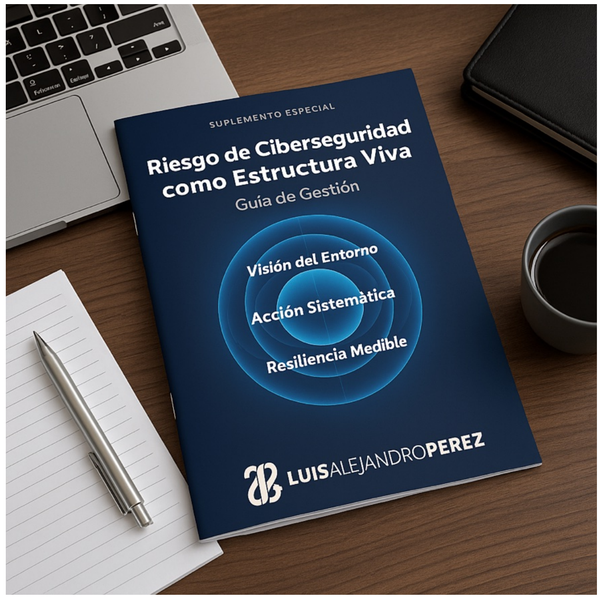
Nuestro enfoque permite hacerlo visible:

- Evalúa la madurez organizacional con base en evidencias.
- Integra el desempeño operativo, financiero y humano.
- Relaciona inversión, valor protegido y capacidad de respuesta.
- Demuestra que la continuidad es rentable, cuando se gestiona con criterio.

Una buena estrategia sin métricas claras
termina perdiendo coherencia.

No se trata solo de gestionar el riesgo.

Se trata de cómo decides frente a él.



Iniciar conversación

LUISALEJANDROPEREZ