CSURFACE

GUÍA · CYBER RISK QUANTIFICATION

Guía de implementación de Cuantificación de Riesgo Cibernético

El paso a paso completo para transformar la incertidumbre del riesgo cibernético en exposición financiera mensurable — de la preparación inicial a la metodología FAIR, a las ocho etapas de implementación y al informe que el consejo aprueba.

TEMA	PÚBLICO	EDICIÓN
Cuantificación de Riesgo	CISO · Riesgo · CFO · Comité de Auditoría	2026

LECTURA	CLASIFICACIÓN	FUENTE
~21 páginas	Público	Plataforma CSURFACE

INTRODUCCIÓN

Cuantificar el riesgo es una decisión de gestión

Qué es el CRQ, para quién se escribió esta guía y el recorrido que sigue de la preparación al informe.

Guía 2026
CSURFACE

COSTO MEDIO DE VIOLACIÓN

€3,90M

media en Brasil en 2025 (IBM Cost of a Data Breach)[4]

SANCIÓN ADMINISTRATIVA RGPD

2%

de la facturación por infracción, limitada a €20M

ETAPAS DE IMPLEMENTACIÓN

8

del alcance a la iteración continua, detalladas en esta guía

Cyber Risk Quantification (CRQ) es la disciplina de medir el riesgo cibernético en términos financieros — en euros, en la misma unidad monetaria con que el consejo ya administra capital. En lugar de afirmar que "el riesgo es alto", el CRQ responde a una pregunta que el consejo sabe gestionar: **cuánto debe perder la organización, por año, como consecuencia de incidentes cibernéticos**, y cuál es el peor caso razonable de esa pérdida.

La respuesta llega en forma de dos magnitudes: la **pérdida anual esperada (ALE)** y el **Value at Risk (VaR)**, generalmente reportado en los percentiles P90 y P99. Son las mismas magnitudes con las que la tesorería, el área de seguros y la auditoría ya trabajan para otros riesgos corporativos. El CRQ simplemente lleva el riesgo cibernético a ese mismo plano.

Esta es la **guía completa de implementación**. El whitepaper de CRQ presenta la tesis en síntesis; este documento es la profundización práctica — destinado a quien necesita montar y sostener el programa.

Para quién es esta guía. Para el **CISO** que necesita defender el presupuesto; para el área de **Riesgo** que integra lo cibernético al mapa corporativo; para el **CFO** que dimensiona reservas y seguro; y para el **comité de auditoría** que necesita una trilla defensable ante el regulador.

Qué cubre esta guía

- Los **obstáculos** a superar antes de iniciar el programa.
- Por qué la **matriz cualitativa 5×5** falla como instrumento de decisión.
- La metodología **FAIR** y su descomposición del riesgo.
- Las **ocho etapas** de implementación, detalladas una a una.
- Buenas prácticas, trampas y un **ejemplo trabajado** reproducible en la calculadora pública.

PARTE 01 · PREPARACIÓN

Los obstáculos a superar antes de comenzar

Siete precondiciones que determinan si el programa de CRQ entrega valor o si se traba en el camino.

Guía 2026
CSURFACE

El éxito de un programa de cuantificación depende de la preparación, más que de la fórmula. Antes de modelar la primera variable, conviene verificar si las siete condiciones a continuación están mínimamente satisfechas. Ninguna necesita estar perfecta; todas necesitan estar atendidas.

Las siete precondiciones

1. **Inventario de activos confiable.** No se cuantifica lo que no se conoce. Un inventario incompleto produce una exposición subestimada — y una falsa sensación de control.
2. **Datos y telemetría mapeados.** Identificar las fuentes es prioridad: costo de incidentes pasados, tiempo de indisponibilidad, multas regulatorias y *breach intelligence* de mercado. Saber qué datos son relevantes viene antes de recolectarlos.
3. **Lenguaje común.** Seguridad opera en CVE y CVSS; el consejo delibera en euros y EBITDA. Sin esa traducción formal, el programa no obtiene adhesión del liderazgo y pierde patrocinio antes de producir resultado.
4. **Calibración de estimaciones.** En ausencia de datos históricos, recurra a estimaciones de especialistas estructuradas como intervalos de confianza calibrados, que preservan la incertidumbre de la estimación. Un intervalo bien calibrado refleja la realidad del riesgo con más fidelidad que un número exacto desprovisto de fundamento.
5. **Apetito de riesgo en términos financieros.** ¿Cuánta exposición anual, en euros, tolera el consejo? Sin ese límite definido, no hay referencia contra la cual comparar el resultado del modelo.
6. **Evitar los dos errores opuestos.** De un lado, la falsa precisión — un número exacto presentado sin intervalo de incertidumbre. Del otro, la parálisis de aguardar la implementación del "FAIR completo" (12 meses o más) antes de entregar cualquier resultado. El enfoque correcto es iniciar con alcance restringido y rigor metodológico, expandiendo gradualmente a medida que el programa demuestra valor.
7. **Equipo multifuncional.** El CRQ no es un programa exclusivo del área de seguridad. Su ejecución requiere la participación de riesgo, seguridad, finanzas y unidades de negocio — cada función aporta una parte insustituible de los datos y del juicio especializado.

El error de partida más común. Tratar la cuantificación como un ejercicio técnico aislado del área de seguridad. Sin finanzas a la mesa, faltan los datos de costo; sin riesgo corporativo, el resultado no llega al mapa de riesgos; sin patrocinio del consejo, el programa no sobrevive al primer trimestre. La composición del equipo es una decisión estratégica de primer orden.

Principio orientador. La madurez en CRQ es un proceso de avance incremental. Iniciar con alcance restringido, atendiendo parcialmente las siete precondiciones, produce resultados más pronto y con mayor adherencia a la realidad operativa que aguardar condiciones ideales que raramente se concretan.

PARTE 02 · EL PROBLEMA DE LO CUALITATIVO

Por qué la matriz 5×5 falla como dato

Tres fallas estructurales de la matriz de riesgo rojo-amarillo-verde — con ejemplos concretos.

La matriz de riesgo 5×5 es popular por su simplicidad. Pero la investigación académica sobre el instrumento — en especial el trabajo de Anthony (Tony) Cox[2] y la crítica de Douglas Hubbard[3] a los *heat maps* — muestra que esa simplicidad esconde defectos que comprometen la decisión. Esta página trata de las tres primeras fallas; la siguiente concluye la crítica.

Falla 1 — Resolución pobre y compresión de rango

Una matriz 5×5 tiene apenas **25 celdas** para representar un universo continuo e ilimitado de riesgo. Riesgos cuantitativamente muy distintos son asignados a la misma celda. La investigación de Tony Cox muestra que matrices típicas comparan correctamente **menos del 10% de los pares de riesgos**.

> **Ejemplo.** Un riesgo de exposición de aproximadamente **€ 200 mil/año** y otro de cerca de **€ 8 millones/año** pueden ambos ser etiquetados "Alto" en la misma celda. Para el consejo, son el mismo riesgo — y el capital de remediación se asigna de forma equivocada, sin que el desvío se perciba.

Falla 2 — Inversión de riesgo y reversión de ranking

Cuando probabilidad e impacto están **negativamente correlacionados**, la matriz puede atribuir la categoría **mayor** al riesgo cuantitativamente **menor**. Cox concluye que, en esos casos, la matriz es "peor que inútil" — invierte activamente la prioridad correcta.

> **Ejemplo.** Compare un evento raro de impacto altísimo (un fraude catastrófico improbable) con un evento frecuente de impacto moderado. Según los bordes de los rangos, la matriz puede clasificar el segundo como más grave que el primero — cuando el primero tiene una pérdida anual esperada mayor.

Falla 3 — Subjetividad e inconsistencia

¿"Probabilidad alta" significa 30%? ¿70%? Sin escalas numéricas definidas, cada evaluador interpreta las etiquetas de manera distinta. El **mismo riesgo recibe celdas diferentes** según quién complete la matriz.

El resultado es que la matriz registra opinión en lugar de dato verificable. Y la opinión no es auditable, no es comparable entre áreas y no sobrevive a la rotación de quien la produjo.

> **Ejemplo.** Dos analistas evalúan el mismo riesgo de indisponibilidad. Uno, conservador, marca "Probabilidad media"; el otro, recién salido de un incidente parecido, marca "Alta". La matriz mueve el riesgo de un color a otro — y nada en la realidad del riesgo cambió.

El hilo conductor. Las tres fallas tienen la misma raíz: la matriz sustituye la magnitud por una etiqueta. Las etiquetas no tienen aritmética, no tienen escala y no tienen unidad. Sin eso, no hay manera de que el instrumento sostenga una decisión de capital.

PARTE 02 · EL PROBLEMA DE LO CUALITATIVO (CONT.)

La matriz no agrega ni dialoga

Las tres fallas finales — y lo que el consejo pierde cuando el riesgo llega solo coloreado.

Falla 4 — La matriz no agrega

Dos riesgos "Altos" no suman a "Muy Alto" de forma coherente — no hay aritmética detrás de los colores. No es posible sumar la exposición de un **portafolio entero de riesgos** dentro de una matriz.

> **Ejemplo.** El consejo pregunta: "¿Cuál es nuestra exposición cibernética total?" Con 30 riesgos dispersos por la matriz, la única respuesta posible es un recuento de colores — "tenemos 8 rojos". El total financiero, que es lo que el consejo pidió, la matriz no lo proporciona.

Falla 5 — Sesgo de centralización

Los evaluadores tienden a evitar los extremos de las escalas y a agrupar casi todo en las celdas del medio. La matriz **pierde poder de discriminación** justamente donde más lo necesitaría.

> **Ejemplo.** En un inventario de 40 riesgos, 32 se clasifican como "Medio/Medio". La matriz que debería priorizar pasa a homogeneizar — y el área de seguridad vuelve a decidir por instinto qué riesgo tratar primero.

Falla 6 — No dialoga con el apetito de riesgo

El consejo define tolerancia en **euros**: "no aceptamos una exposición anual por encima de € X". La etiqueta "Alto" no se compara con ese límite financiero — está en una escala diferente, sin puente entre ambas.

> **Ejemplo.** El apetito aprobado es de € 5 millones de exposición anual. La matriz señala "3 riesgos Altos". Es imposible decir si la organización está dentro o fuera del apetito — el instrumento y el límite no se hablan.

Conclusión de las seis fallas. La matriz cualitativa tiene un uso legítimo: *triaje inicial* de riesgos recién identificados, cuando aún no hay ningún dato. El error está en tratarla como la respuesta financiera que el consejo espera. Para decisión de capital, debe ceder lugar a un modelo cuantitativo.

ATENCIÓN **La matriz comunica**
Prioridad relativa gruesa entre riesgos ya conocidos — útil como punto de partida.

CRÍTICO **La matriz no comunica**
Magnitud, agregación de portafolio, trade-off de capital ni comparación con el apetito de riesgo.

PARTE 03 · LA METODOLOGÍA

FAIR: descomponer el riesgo para poder calcularlo

El estándar abierto que transforma el riesgo opaco en variables observables y calculables.

Guía 2026
CSURFACE

LA DESCOMPOSICIÓN DEL FAIR · DEL RIESGO OPACO A LA VARIABLE CALCULABLE

1. **Riesgo** — Frecuencia de eventos de pérdida × Magnitud de la pérdida — el todo, descompuesto.
2. **Frecuencia** — Frecuencia de evento de amenaza × Vulnerabilidad — la probabilidad anual de pérdida.
3. **Magnitud** — Pérdida primaria + Pérdida secundaria — el costo esperado por evento.
4. **Distribución** — Cada variable se convierte en un rango probabilístico para la simulación.
5. **Monte Carlo** — Miles de simulaciones generan ALE y VaR (P50 / P90 / P99).

El principio: separar y cuantificar

El **FAIR — Factor Analysis of Information Risk**[1] es un estándar abierto que descompone el riesgo en variables observables, en lugar de tratarlo como un todo opaco. La ecuación central es simple:

Riesgo = Frecuencia de eventos de pérdida × Magnitud de la pérdida
Frecuencia = Frec. de evento de amenaza × Vulnerabilidad
Magnitud = Pérdida primaria + Pérdida secundaria

La **frecuencia de evento de amenaza** es cuántas veces, por año, un agente intenta alcanzar el activo. La **vulnerabilidad** es la probabilidad de que el intento tenga éxito. La **pérdida primaria** es el costo directo del incidente; la **secundaria** incluye multas, pérdida de clientes y daño de marca.

Distribuciones en vez de puntos únicos

El diferencial del FAIR es que cada variable se estima como una **distribución de probabilidad** — un rango con mínimo, máximo y valor más probable — en lugar de un número exacto. Esto reconoce la incertidumbre inherente al riesgo, en lugar de esconderla.

Sobre esas distribuciones opera la **simulación de Monte Carlo**: miles de escenarios muestreados a partir de los rangos probabilísticos, cuyo resultado agregado es una curva de pérdida. De esa curva se extraen el **ALE** (pérdida anual esperada, el valor medio) y el **VaR** en los percentiles P50, P90 y P99 — el peor caso razonable.

El FAIR organiza el juicio técnico en una estructura auditable. Cada estimación queda explícita, documentada y revisable. Cuando un número es cuestionado por la auditoría, es posible mostrar exactamente de qué variable y de qué rango provino. Es esa trazabilidad la que hace el resultado defensable.

PARTE 04 · IMPLEMENTACIÓN

Las ocho etapas del programa de CRQ

Visión general del recorrido — del alcance inicial a la iteración continua.

EL RECORRIDO DE IMPLEMENTACIÓN · OCHO ETAPAS

1 **Alcance**
Definir las preguntas a responder.

→

2 **Framework**
Elegir la metodología — FAIR.

→

3 **Inventario**
Mapear y valorar los activos.

→

4 **Datos**
Recolectar telemetría e histórico.

5 **Modelar**
Descomponer y estimar distribuciones.

→

6 **Simular**
Monte Carlo, ALE y VaR.

→

7 **Comunicar**
Traducir al lenguaje del board.

→

8 **Iterar**
Recalibrar de forma continua.

Cuadro-resumen de las ocho etapas

#	ETAPA	ENTREGA PRINCIPAL
1	Alcance y objetivos	Las preguntas que el informe debe responder
2	Elección del framework	FAIR adoptado como base metodológica
3	Inventario y valoración	Lista de activos con valor de negocio
4	Recolección de datos	Telemetría de amenaza, controles e histórico
5	Modelado	Variables FAIR estimadas como distribuciones
6	Simulación	**ALE y VaR (P50 / P90 / P99)**
7	Comunicación	Informe financiero para el board
8	Iteración	Recalibración continua del modelo

Un ciclo iterativo de alcance creciente. Las ocho etapas describen un ciclo iterativo. La primera ejecución puede cubrir un único activo crítico en pocas semanas; las iteraciones subsecuentes amplían el alcance y refinan las estimaciones. El programa consolida madurez a cada ciclo concluido, en avance continuo.

Cómo leer las próximas páginas

Cada una de las **ocho etapas** ocupa una página dedicada — con el objetivo, el paso a paso ejecutable, los insumos necesarios y el error común a evitar. La simulación, por su densidad, ocupa dos páginas.

Un **caso trabajado único** — la cuantificación del riesgo de e-commerce de una red minorista — atraviesa las ocho etapas, con números reales en cada etapa, del alcance inicial al informe llevado al consejo.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 1 DE 8

Etapa 1 · Alcance y objetivos

Declarar la decisión que el número va a sostener y recortar el primer escenario de riesgo a cuantificar.

Guía 2026
CSURFACE

Objetivo de la etapa. Concluir con tres definiciones registradas: la **decisión-objetivo** que el informe debe sostener, las **preguntas de negocio** a responder y un **escenario de riesgo único** — un par agente × activo — elegido para la primera iteración.

Cómo ejecutar — paso a paso

1. **Identifique la decisión.** La cuantificación es, en la práctica, insumo de una decisión. Aprobar un presupuesto de remediación, dimensionar el seguro cibernético o aceptar formalmente un riesgo son decisiones distintas, y cada una exige un recorte diferente. Nombre la decisión antes de cualquier cálculo.
2. **Escriba las preguntas en lenguaje de negocio.** "¿Cuál es la exposición anual, en euros, de este escenario?" "¿La inversión prevista reduce la exposición más de lo que cuesta?" Las preguntas formuladas en términos técnicos producen informes técnicos, y no decisiones de gestión.
3. **Recorte un escenario de riesgo único.** No se cuantifica "el riesgo cibernético" como un todo. La unidad de análisis del FAIR es el escenario: un **agente de amenaza** específico, actuando sobre un **activo** específico, produciendo una **forma de pérdida** específica.
4. **Fije el horizonte y la unidad.** El estándar de mercado es una ventana de 12 meses, con resultado en euros. Toda variable estimada y todo número reportado pasan a obedecer ese recorte.
5. **Nombre al patrocinador.** La decisión-objetivo necesita un responsable en el nivel adecuado — CFO o comité de auditoría. Sin patrocinio ejecutivo declarado, el resultado no se convierte en deliberación.

En el caso · la minorista

El ejemplo trabajado de esta guía acompaña una **red minorista** — € 1,2 mil millones de facturación anual, e-commerce propio responsable de cerca de € 28 millones de ingresos por mes.

Decisión-objetivo: aprobar, o no, una inversión de **€ 1,2 millón** en WAF gestionado y hardening de la aplicación de e-commerce.

ESCENARIO ELEGIDO PARA LA 1ª ITERACIÓN	
Agente de amenaza	**Atacante externo**
Activo	**Aplicación de e-commerce**
Forma de pérdida	**Exfiltración de datos de clientes**
Horizonte · unidad	**12 meses · €**

Error común. Iniciar por la elección de herramientas y sistemas antes de definir la pregunta de negocio. Sin claridad sobre lo que el informe debe responder — y para quién —, el programa produce análisis técnicamente correctos que no fundamentan ninguna decisión de gestión.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 2 DE 8

Etapa 2 · Elegir el framework

Adoptar una metodología estandarizada, la herramienta de simulación y el estándar de documentación.

Objetivo de la etapa. Adoptar el **FAIR** como taxonomía, elegir la **herramienta de simulación** adecuada a la etapa de madurez del programa y fijar el **estándar de documentación** que hará cada estimación auditable.

Cómo ejecutar — paso a paso

1. **Adopte el FAIR como taxonomía.** El *Factor Analysis of Information Risk* es un estándar abierto, mantenido por el FAIR Institute, compatible con ISO 27005 y COSO ERM. Adoptarlo da al programa un vocabulario común y una descomposición ya consolidada.
2. **Liste las variables que el modelo exige.** El FAIR descompone el riesgo en cinco variables a estimar: Frecuencia de Evento de Amenaza, Vulnerabilidad, Pérdida Primaria, Frecuencia de Pérdida Secundaria y Pérdida Secundaria. Son ellas las que las etapas siguientes van a alimentar.
3. **Elija la herramienta de simulación.** Para la primera iteración, una planilla con función de Monte Carlo es suficiente. A medida que el alcance crece, herramientas dedicadas — FAIR-U, bibliotecas open-source o un módulo de CRQ — ganan eficiencia y reducen el error operativo.
4. **Defina el estándar de documentación.** Cada estimación registra fuente, rango, autor y fecha — una *ficha de variable*. Es esa trilla la que permite, ante un cuestionamiento de la auditoría, mostrar de qué dato y de qué rango derivó un número.
5. **Concilie con lo que ya existe.** Mapee el FAIR al ISO 27005 y al COSO ERM ya adoptados, para que el resultado entre en el mapa de riesgos corporativo sin retrabajo ni terminología concurrente.

Por qué un estándar abierto

Un framework estandarizado y documentado es lo que hace el resultado **reproducible** — otra persona, con los mismos datos, llega al mismo número — y **comparable** a lo largo del tiempo. Un método propio y no documentado no ofrece ninguna de las dos garantías.

En el caso · la minorista

La minorista adopta el **FAIR**. Para el primer ciclo, la herramienta es una **planilla de Monte Carlo** de 100.000 iteraciones. La documentación sigue el modelo de una ficha por variable, y el resultado será reflejado en el mapa de riesgos corporativo ya mantenido bajo ISO 27005.

Error común. La adopción de un método propio y no documentado. Tal enfoque compromete la auditabilidad y la reproducibilidad de los resultados, impide la comparación consistente a lo largo del tiempo y no se sostiene en el largo plazo, por la falta de adherencia a normas y estándares de mercado.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 3 DE 8

Etapa 3 · Inventario y valoración

Listar los activos que componen el escenario y atribuir a cada uno su valor de negocio.

Objetivo de la etapa. Producir la lista completa de los activos que sostienen el escenario, cada uno con un **valor de negocio** — cuánto pierde la organización si ese activo es comprometido, distinto de su valor contable.

Cómo ejecutar — paso a paso

1. **Liste los activos que componen el escenario.** No solo la aplicación visible: todo lo que la sostiene — servidores, bases de datos, APIs, integraciones y componentes de terceros embebidos en el código.
2. **Registre lo que cada activo sostiene.** El ingreso que viabiliza, los datos que procesa, la función operativa que desempeña. Ese registro es la base de la valoración.
3. **Valore por la pérdida.** El valor de negocio corresponde a la pérdida derivada del compromiso del activo: ingreso interrumpido por día de indisponibilidad, número de registros de datos personales expuestos, costo de reconstrucción. El valor contable es una referencia diferente, impropia para esa finalidad.
4. **Marque la dependencia externa.** Los componentes de terceros integrados al activo entran en el inventario — son superficie cuya responsabilidad recae sobre la organización, independientemente de la autoría del código.
5. **Verifique la completitud.** El activo ausente del inventario es el que subestima toda la exposición. Un inventario derivado de descubrimiento continuo de la superficie externa reduce ese punto ciego de forma estructural.

En el caso · la minorista

Los activos que componen el escenario de e-commerce y el valor de negocio de cada uno:

ACTIVO	SOSTIENE	VALOR DE NEGOCIO
Aplicación de e-commerce	Canal de venta online	**€ 28 mi ingreso/mes**
Base de datos de clientes	Registro e histórico	**2,3 mi de registros PII**
Gateway de pago	Transacciones con tarjeta	**Alcance PCI-DSS**
3 APIs públicas	App móvil y socios	**Superficie de entrada**

Error común. La adopción de un inventario incompleto como base de cálculo. Los activos expuestos ausentes del relevamiento producen exposición sistemáticamente subestimada — comprometiendo la validez del modelo y la credibilidad del informe ante la auditoría.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 4 DE 8

Etapa 4 · Recolectar datos y telemetría

Reunir los insumos que van a calibrar cada una de las cinco variables del modelo FAIR.

Objetivo de la etapa. Para cada variable del FAIR, identificar y reunir la fuente de dato que la calibra — priorizando el dato interno y completando, donde falta, con referencias de mercado y estimaciones calibradas.

Cómo ejecutar — paso a paso

1. **Mapee la fuente de cada variable antes de recolectar.** Saber qué dato calibra qué variable evita una recolección dispersa, que reúne mucho dato sin alimentar el modelo.
2. **Reúna el dato de frecuencia.** La Frecuencia de Evento de Amenaza y la Vulnerabilidad provienen de logs de WAF e IDS, inteligencia de amenazas, resultados de pruebas de intrusión, de la postura de parches y de la explotabilidad conocida de las fallas expuestas.
3. **Reúna el dato de magnitud.** La Pérdida Primaria y Secundaria provienen del costo de incidentes pasados, de contratos de respuesta a incidente, del histórico sectorial de sanciones RGPD y de referencias de mercado.
4. **Priorice el dato interno.** El dato propio — un incidente ya ocurrido, un costo ya calculado — es el más valioso. Agótelo antes de recurrir a referencias externas.
5. **Donde falte dato, calibre la estimación.** La ausencia de histórico no interrumpe el programa: registre un rango de especialista calibrado en lugar de un número exacto sin fundamento.

Dónde se calibra cada variable

VARIABLE FAIR	FUENTE DE DATO	INSUMO DE CSURFACE
Frec. Evento de Amenaza	Logs WAF/IDS · threat intel	**Threat sensor — actividad real de amenaza**
Vulnerabilidad	Pentest · postura de parches	**Inteligencia de exploits · explotabilidad**
Pérdida Primaria	Incidentes pasados · contratos IR	—
Pérdida Secundaria	Histórico RGPD · churn · IBM 2025	—

El threat sensor y la inteligencia de exploits de CSURFACE alimentan directamente los dos insumos más difíciles de estimar — la frecuencia de amenaza y la vulnerabilidad. Detalle en la página 17.

Calibración — qué es. Calibrar una estimación es entrenar al especialista para proporcionar un intervalo dentro del cual el valor real cae con 90% de confianza. Es una habilidad entrenable: un especialista calibrado produce rangos confiables incluso en ausencia de dato histórico.

Error común. Condicionar el avance del programa a la disponibilidad de datos completos. La ausencia de datos históricos internos no impide el modelado — impide únicamente el modelado sin calibración.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 5 DE 8

Etapa 5 · Modelar las distribuciones

Convertir cada variable del FAIR en una distribución de probabilidad de tres puntos.

Objetivo de la etapa. Transformar cada una de las cinco variables en una **distribución** — mínimo, valor más probable y máximo —, registrando la fuente de cada punto. Es el conjunto de esas distribuciones lo que la simulación va a procesar.

Por qué una distribución en vez de un número

Un valor único descarta la incertidumbre — y la incertidumbre *es* el dato más importante del riesgo. Una distribución de tres puntos declara, de forma explícita, lo que se sabe y lo que no se sabe sobre cada variable.

La mayoría de las variables del FAIR se modela como una distribución **PERT (BetaPERT)**: una curva suave, anclada en el valor más probable y limitada por el mínimo y el máximo. Su media es **(mín + 4 × más probable + máx) ÷ 6**.

Cómo ejecutar — paso a paso

1. **Defina el intervalo de 90%.** El mínimo y el máximo que cercan el 90% de la probabilidad — no el peor caso absoluto imaginable.
2. **Agregue el valor más probable.** El punto en que la estimación se concentra, entre el mínimo y el máximo.
3. **Elija la forma.** PERT para la mayoría de las variables; una forma de cola más larga, como la lognormal, para magnitudes de pérdida con cola pesada.
4. **Someta a revisión multifuncional.** Riesgo, seguridad y finanzas validan los rangos antes de que la simulación sea ejecutada.

En el caso · las cinco distribuciones de la minorista

VARIABLE	MÍN	PROBABLE	MÁX
Frec. Evento de Amenaza	2	5	14 /año
Vulnerabilidad	3%	8%	20%
Pérdida Primaria	0,9	2,4	6,0 mi
Frec. Pérdida Secundaria	70%	90%	100%
Pérdida Secundaria	1,5	6,0	22,0 mi

Frec. de Evento de Amenaza en intentos calificados por año. Pérdidas en € millones. Fuentes: logs de WAF, prueba de intrusión, incidente interno de 2023 e IBM Cost of a Data Breach 2025.

Error común. Sustituir distribuciones por valores puntuales. Esa simplificación elimina la representación explícita de la incertidumbre — característica que confiere al modelo tanto su honestidad técnica como su defensabilidad ante el comité de auditoría.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 6 DE 8 · PARTE 1

Etapa 6 · Simular — el método de Monte Carlo

Qué hace la simulación, por qué es necesaria y cómo opera su algoritmo.

Guía 2026
CSURFACE

Qué es la simulación de Monte Carlo

Monte Carlo es una técnica que **ejecuta el modelo miles de veces**. En cada ejecución, sortea un valor de cada distribución de entrada y calcula la pérdida de esa ejecución. El conjunto de todos los resultados forma la **curva de pérdida anual** — la distribución completa de los resultados posibles.

Por qué es necesaria

No es posible sumar y multiplicar cinco distribuciones de probabilidad analíticamente, a mano. Un cálculo de punto único — multiplicar solo los valores medios — **descarta la incertidumbre** y devuelve un número que esconde el rango de resultados. La simulación propaga la incertidumbre de cada entrada hasta el resultado final.

EL ALGORITMO · UN "AÑO POSIBLE" POR ITERACIÓN

1 — Sortee frecuencia
Sortee la Frec. de Evento de Amenaza y la Vulnerabilidad. El producto es λ — eventos de pérdida esperados en el año.

→

2 — Cuente los eventos
Una distribución de Poisson con media λ convierte la frecuencia esperada en un conteo entero: 0, 1, 2…

→

3 — Componga la pérdida
Para cada evento, sortee la Pérdida Primaria; por la Frec. de Pérdida Secundaria, decida si hay pérdida secundaria y sortéela.

4 — Sume el año
La suma de las pérdidas de los eventos es la pérdida total de ese año simulado.

→

5 — Repita
De 10.000 a 100.000 veces. Cada repetición es un año posible, independiente de los demás.

→

6 — Agregue
La media de las pérdidas anuales es el ALE; los percentiles de la curva son el VaR.

Cuántas iteraciones. Diez mil iteraciones bastan para una lectura estable de la media (ALE). Para que la cola — el VaR P99 — quede precisa, se recomiendan 100.000. En el ejemplo de la minorista, la simulación corrió **100.000 iteraciones** sobre las cinco distribuciones de la etapa 5.

Una iteración ilustrada — un año posible

Para hacer concreto el algoritmo, acompañe una única iteración de la simulación de la minorista:

1 · Sorteo de frecuencia	**Amenaza 6,1 × Vuln. 10,5% → λ = 0,64**
2 · Conteo · Poisson (λ = 0,64)	**1 evento en este año**
3 · Pérdida del evento	**Primaria € 2,1 mi + Secundaria € 7,4 mi**
4 · Pérdida del año	**€ 9,5 mi**

Esta iteración contribuye con **€ 9,5 millones**. La iteración siguiente, con un λ menor, puede sortear **cero eventos** y contribuir con € 0. La media de 100.000 iteraciones como esta es el ALE; el ordenamiento de todas ellas, de la menor a la mayor, produce la curva de pérdida de la próxima página.

Por qué una distribución de Poisson

La frecuencia λ es una **media** — pero el número de incidentes en un año concreto es un entero: 0, 1, 2. La distribución de Poisson es el instrumento estadístico que convierte una tasa media de eventos independientes en la probabilidad de cada conteo posible.

Con el λ medio de **0,55** del escenario de la minorista, la Poisson atribuye cerca de **58%** de probabilidad a ningún evento en el año, **32%** a exactamente uno y **10%** a dos o más. Es esa asimetría — la mayoría de los años sin pérdida, unos pocos con pérdida elevada — la que moldea el resultado de la etapa.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 6 DE 8 · PARTE 2

Etapa 6 · Simular — ALE y VaR del caso

Leer el resultado de la simulación: la pérdida media, la cola y la curva de excedencia.

ALE · PÉRDIDA ANUAL ESPERADA
€ 5,3 mi
la media de la curva de pérdida

VAR · PERCENTIL 90
€ 16,8 mi
el número para decisión de capital

VAR · PERCENTIL 99
€ 34,4 mi
el peor caso razonable

Curva de excedencia · la minorista

La probabilidad de que la pérdida anual del escenario de e-commerce supere cada umbral — la traducción de la incertidumbre en números de decisión:

Cómo leer el resultado

ALE — € 5,3 mi. La pérdida media anual del escenario. Es el valor para el presupuesto recurrente de riesgo y el punto de comparación con el apetito aprobado por el consejo.

VaR P90 — € 16,8 mi. En 1 de cada 10 años, la pérdida supera ese valor. Es la referencia para decisiones de capital y para la priorización de remediaciones.

VaR P99 — € 34,4 mi. El peor caso razonable. Base para el dimensionamiento de reservas de contingencia y de la cobertura de seguro cibernético.

PERCENTIL DE LA CURVA	PÉRDIDA ANUAL	LECTURA
P50 · mediana	€ 0	mayoría de los años sin pérdida
P75	€ 9,7 mi	1 año en 4 supera este valor
P90	€ 16,8 mi	decisión de capital
P99	€ 34,4 mi	reservas y seguro

La lectura que más sorprende al consejo. En cerca del **60% de los años simulados, la pérdida fue € 0** — el incidente no ocurre. La mediana (P50) del escenario es, por lo tanto, cero. El ALE de € 5,3 millones es una media que incorpora los años en que el incidente de hecho ocurre. Es exactamente por eso que el informe reporta la media y la cola, y nunca la mediana aislada, que sugeriría, falsamente, ausencia de riesgo.

Error común. Reportar exclusivamente la media (ALE) y omitir el análisis de cola. El VaR P99 — el peor caso razonable — es la métrica que fundamenta el dimensionamiento de reservas y la contratación de seguro cibernético; sin él, el informe es incompleto para una decisión de capital.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 7 DE 8

Etapa 7 · Comunicar al consejo

Traducir la curva de pérdida en una recomendación: el número, el apetito y el trade-off de la decisión.

Objetivo de la etapa. Convertir el resultado de la simulación en un informe de una página que el consejo pueda deliberar — abriendo por el número, comparándolo con el apetito de riesgo y exponiendo el trade-off de cada alternativa de remediación.

Cómo ejecutar — paso a paso

1. **Abra por el número.** "La exposición anual de este escenario es de € 5,3 millones; el peor caso razonable es de € 34,4 millones." La metodología va al apéndice.
2. **Compare con el apetito de riesgo.** Posicione la exposición contra el límite, en euros, que el consejo aprobó. Es esa comparación la que indica si hay o no decisión a tomar.
3. **Presente el trade-off.** Cuánto cuesta cada alternativa de remediación y cuánto reduce el ALE. Es lo que transforma un número en una recomendación accionable.
4. **Muestre el rango entero.** El informe expone la incertidumbre — la curva de pérdida —, evitando la falsa precisión de un valor aislado.
5. **Adjunte la trilla.** Las fichas de variable y las premisas van en apéndice, a disposición de la auditoría, fuera del cuerpo principal del informe.

En el caso · la recomendación al consejo

La inversión de **€ 1,2 millón** en WAF gestionado y hardening reduce la Vulnerabilidad del valor más probable de 8% a 3%. El modelo, recalculado, devuelve:

MÉTRICA	HOY	TRAS LA INVERSIÓN
ALE	€ 5,3 mi	**€ 2,0 mi**
VaR P90	€ 16,8 mi	**€ 9,8 mi**
VaR P99	€ 34,4 mi	**€ 21,4 mi**

La frase para el consejo. "La inversión de € 1,2 millón reduce la exposición anual en € 3,3 millones — de € 5,3 mi a € 2,0 mi — y el peor caso razonable en € 13 millones. El retorno se da ya en el primer año. Recomendación: aprobar." Una remediación se justifica cuando reduce el ALE por más de lo que cuesta.

Error común. Presentar la metodología y los parámetros del modelo en lugar del resultado y de la recomendación. El consejo necesita la exposición en euros y el análisis de costo-beneficio; la descripción del proceso permanece en el apéndice.

PARTE 04 · IMPLEMENTACIÓN · ETAPA 8 DE 8

Etapa 8 · Iterar y recalibrar

Mantener el número válido conforme la realidad cambia — y ampliar el alcance a cada ciclo.

Objetivo de la etapa. Establecer el ciclo de recálculo que mantiene el ALE adherente al riesgo vigente — confrontando lo previsto con lo ocurrido, reajustando las distribuciones y ampliando el alcance para el próximo escenario.

Cómo ejecutar — paso a paso

1. **Defina los disparadores de recálculo.** Un cambio material en el inventario, una nueva amenaza relevante, un control implantado o el cierre de un trimestre disparan la revisión del modelo.
2. **Confronte lo previsto con lo ocurrido.** ¿Hubo evento en el período? ¿El costo calculado cayó dentro del rango estimado? Ese confronte es el backtesting que valida — o corrige — el modelo.
3. **Reajuste las distribuciones.** Cada nuevo dato estrecha un rango antes amplio. El modelo gana precisión a cada ciclo concluido.
4. **Amplíe el alcance.** Con el primer escenario consolidado, el próximo entra en la fila. La suma de los escenarios cuantificados forma la exposición cibernética de portafolio.
5. **Versione cada informe.** Fecha, premisas y resultado de cada ciclo quedan registrados — la trilla que demuestra la evolución del riesgo a lo largo del tiempo.

En el caso · la minorista

Implantado el WAF gestionado, la minorista define el **recálculo trimestral** del escenario de e-commerce. En el primer trimestre tras la remediación, la Vulnerabilidad observada en los logs confirma la caída proyectada, y el ALE recae al rango previsto de **€ 2,0 millones**.

El confronte entre lo previsto y lo ocurrido — ningún evento de pérdida en el período, costos dentro del rango estimado — valida el modelo. Las distribuciones se reajustan con los nuevos datos, y el rango de cada variable se estrecha.

Con el primer escenario consolidado, el **próximo entra en el alcance**: el compromiso del ERP por ransomware. Recorre las mismas ocho etapas. La suma de los escenarios cuantificados pasa a formar la **exposición cibernética de portafolio** — el número que el consejo compara con el apetito de riesgo corporativo.

Por qué el número necesita ser vivo. Un ALE calculado hace 12 meses describe un estado anterior del inventario, de las amenazas y de los controles, desfasado respecto al perfil de riesgo vigente. La recalibración periódica es la condición que mantiene el número válido como base de decisión a lo largo del tiempo.

Error común. Tratar el primer informe como referencia permanente. El inventario se expande, nuevas vulnerabilidades surgen y se implantan controles — la recalibración periódica es condición de validez del número.

El ciclo se cierra — y recomienza. Concluida la octava etapa, el programa recomienza en lugar de terminar. Las ocho etapas forman un ciclo, y cada vuelta amplía el alcance, estrecha las distribuciones y mejora la precisión del número. Las próximas páginas reúnen las buenas prácticas y las trampas que distinguen un ciclo que sostiene decisiones de uno que produce números frágiles.

PARTE 05 · EJECUCIÓN

Buenas prácticas y trampas a evitar

Lo que separa un programa de CRQ que sostiene decisiones de uno que produce números frágiles.

Buenas prácticas

1. **Comience pequeño.** Cuantifique primero un único activo o riesgo crítico. Un resultado de alcance restringido, metodológicamente consistente y defensable, tiene más valor institucional que un plan abarcador que no se concreta.
2. **Priorice los datos ya disponibles.** Telemetría de seguridad, registros de incidentes, datos financieros y referencias de mercado ya están accesibles — agote esas fuentes antes de estructurar recolecciones adicionales.
3. **Comunique siempre en euros.** El resultado obtiene adhesión del liderazgo cuando se presenta en la magnitud con que este toma decisiones. CVE y CVSS deben traducirse en exposición financiera — sin excepción.
4. **Monitoree y refine.** Revise las estimaciones conforme llegan nuevos datos. El modelo gana precisión a cada ciclo — siempre que sea sistemáticamente revisitado.
5. **Mantenga el equipo multifuncional.** Riesgo, seguridad, finanzas y unidades de negocio reunidos — condición necesaria para que el número sea completo y para que la recomendación sea aceptada por las partes que necesitan actuar sobre ella.

Trampas a evitar

CRÍTICO **Falsa precisión**

Presentar un número exacto — "la exposición es € 11.137.482" — sin el rango de incertidumbre. Un intervalo honesto es más confiable que un punto preciso y falso.

CRÍTICO **El "big bang" de 12 meses**

Intentar implementar el FAIR completo, en todo el alcance, antes de entregar cualquier valor. El programa pierde patrocinio mucho antes del primer resultado.

ATENCIÓN **Datos malos, falsa seguridad**

Alimentar el modelo con inventario incompleto o estimaciones no calibradas. El resultado parece sólido, pero describe una realidad que no existe.

El equilibrio. La eficacia del CRQ reside entre dos extremos simétricos: la falsa precisión de un número exacto sin intervalo de incertidumbre y la parálisis derivada de aguardar un programa sin lagunas antes de producir cualquier resultado. Un intervalo bien calibrado, entregado sobre alcance restringido y refinado a cada ciclo, es la trayectoria que confiere credibilidad duradera al programa.

PARTE 06 · EL ENFOQUE CSURFACE

Cómo CSURFACE alimenta el framework

La plataforma provee los dos insumos más difíciles del FAIR: el inventario y la frecuencia de amenaza.

EL CUELLO DE BOTELLA DEL FAIR

Datos de entrada

- Inventario desactualizado
- Frecuencia de amenaza estimada sin calibración
- Recalibración anual

→

LO QUE CSURFACE APORTA AL MODELO

Insumos vivos y continuos

- Inventario del descubrimiento continuo
- Frecuencia calibrada por el threat sensor
- Actividad real de amenazas
- Inteligencia de exploits
- Indicadores de campaña
- Recalibración continua

El inventario proviene del descubrimiento continuo

La etapa 3 — inventario y valoración — es, en la práctica, donde la mayoría de los programas tropieza: no se cuantifica lo que no se conoce. CSURFACE resuelve ese cuello de botella en el origen. El **descubrimiento continuo de la superficie externa** mantiene el inventario de activos actualizado de forma permanente, con Machine Learning para clasificación y atribución de criticidad.

Esto significa que el modelo de CRQ parte de un **inventario vivo** en lugar de una planilla estática que envejece. Cada nuevo activo descubierto entra automáticamente en el alcance del cálculo.

La frecuencia de amenaza proviene del threat sensor

La variable más difícil de estimar en el FAIR es la **frecuencia de evento de amenaza**. CSURFACE la calibra con el **threat sensor**, que observa **actividad real de amenazas**: intentos de explotación, inteligencia de exploits, indicadores de campaña, parámetros, métricas e integraciones.

Esa calibración va **mucho más allá** de CVSS, de los índices de probabilidad de explotación y de los catálogos de explotación activa — esos scores figuran como insumos entre varios. Lo que pesa es la señal en vivo de amenaza observada contra activos como los de la organización.

La calculadora pública y el módulo integrado. La calculadora pública de riesgo es la puerta de entrada: una primera lectura de exposición con pocos parámetros. El **módulo CRQ integrado** sustituye las estimaciones sectoriales por el inventario real y mantiene el **loop cerrado** — el ALE se recalcula a cada cambio en el inventario, en la amenaza y en la remediación.

PARTE 07 · APLICACIÓN PRÁCTICA

Simule usted mismo — un ejemplo trabajado

Reproduzca este cálculo en la calculadora pública: csurface.io/calculadora-de-risco.html

PÉRDIDA ANUAL ESPERADA (ALE)
€ 11,1 mi
probabilidad ajustada × SLE

VALUE AT RISK · P90
€ 20,5 mi
el número para decisión de capital

EXPOSICIÓN A MULTA RGPD
€ 17,5 mi
sanción potencial ponderada por la probabilidad

Paso a paso en la calculadora

El escenario: una **minorista**, facturación de **€ 1,2 mil millones**, 4.500 colaboradores, 8.700 activos y madurez de seguridad intermedia — la misma organización del caso trabajado en las etapas de esta guía. La calculadora estima la exposición **agregada** de la organización; las etapas descomponen, por la metodología FAIR, un **escenario específico** dentro de esa exposición. Acceda a **csurface.io/calculadora-de-risco.html** e introduzca los parámetros a continuación:

1. **Sector** — seleccione *Minorista*. Define la probabilidad-base y el multiplicador de costo del sector.
2. **Facturación anual** — informe *€ 1,2 mil millones*. Entra en el cálculo del SLE y en el techo de la multa RGPD.
3. **Número de colaboradores** — informe *4.500*. Sirve como parámetro de dimensionamiento del tamaño de la organización.
4. **Número de activos** — informe *8.700*. Ajusta el SLE por el tamaño de la superficie de ataque.
5. **Madurez de seguridad** — seleccione *Intermedia*. Modula la probabilidad ajustada.

La calculadora aplica el modelo recalibrado de CSURFACE y retorna ALE, VaR y exposición regulatoria en segundos, sin registro.

El resultado retornado

MÉTRICA	VALOR	PARA QUÉ SIRVE
Probabilidad ajustada	≈ 56%	Probabilidad anual de incidente
SLE	€ 19,8 mi	Pérdida por evento
ALE	€ 11,1 mi	Presupuesto anual
VaR P90	€ 20,5 mi	Decisión de capital
VaR P99	€ 39,9 mi	Reserva / seguro
Multa RGPD	€ 17,5 mi	Exposición regulatoria

La frase para el consejo. "Nuestra exposición cibernética anual es de € 11,1 millones, con VaR P90 de € 20,5 millones y exposición regulatoria de € 17,5 millones." Es ese enunciado — reproducible en la calculadora pública a partir de los parámetros del ejemplo — el que convierte una presentación técnica en una deliberación de capital.

APÉNDICE

Metodología y fuentes

Las referencias que sustentan esta guía y una nota sobre la naturaleza de las estimaciones.

Referencias

1. **FAIR Institute** — Factor Analysis of Information Risk. Estándar abierto de cuantificación de riesgo en información, base metodológica de esta guía.
2. **Anthony (Tony) Cox** — "What's Wrong with Risk Matrices?", *Risk Analysis*, 2008. Análisis de las limitaciones estructurales de las matrices cualitativas de riesgo.
3. **Douglas Hubbard** — crítica a los *heat maps* y a los métodos cualitativos de evaluación de riesgo, y defensa de la medición cuantitativa.
4. **IBM** — Cost of a Data Breach Report 2025. Costo medio de violación de datos en Brasil: €3,90M.

Nota metodológica

El caso trabajado que atraviesa esta guía — la cuantificación del escenario de e-commerce de una red minorista — se obtuvo por **simulación de Monte Carlo** (100.000 iteraciones) sobre distribuciones FAIR. El ejemplo de la página 19, en la calculadora pública, aplica el modelo recalibrado de CSURFACE, que parte de la media nacional del IBM Cost of a Data Breach 2025. Ambos describen un escenario **ficticio e ilustrativo** — destinado a demostrar el método, con finalidad estrictamente educativa.

El CRQ produce **distribuciones de probabilidad**, que expresan rangos de pérdida con su incertidumbre. ALE y VaR son lecturas de una curva de pérdida simulada; la precisión del resultado depende directamente de la calidad del inventario y de los datos de entrada — de ahí el énfasis de esta guía en la preparación y en la iteración continua.

Frameworks y regulaciones citados. FAIR, Monte Carlo, COSO ERM, ISO 27005, RGPD, BACEN y CVM son metodologías y regulaciones públicas, mencionadas como referencia. Este es un material educativo; no sustituye asesoramiento jurídico o regulatorio específico.

PRÓXIMOS PASOS

De la guía a la práctica: comience con un número en euros

La Cuantificación de Riesgo Cibernético es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. Integrada en una plataforma única, reúne descubrimiento continuo de la superficie externa con Machine Learning, análisis de la cadena digital de proveedores, validación de explotabilidad, inteligencia de amenazas con priorización dinámica, monitoreo de credenciales filtradas y cuantificación financiera de riesgo. Opera de forma enteramente externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM para profundizar el alcance.

Use la calculadora de riesgo

Reproduzca el ejemplo de esta guía: estime el ALE y el VaR de su sector en segundos, sin registro — la puerta de entrada para la cuantificación financiera.

Conozca el módulo CRQ

En una demostración, vea el análisis FAIR aplicado a su inventario real, con el loop cerrado que mantiene el ALE siempre actualizado.

Lea el whitepaper de CRQ

La versión síntesis de este tema, con el modelo cuantitativo de CSURFACE detallado parámetro por parámetro.

Vea su exposición en euros — comience por la calculadora pública de riesgo

Abrir la calculadora de riesgo