CSURFACE

WHITEPAPER · CYBER RISK QUANTIFICATION

Convirtiendo el riesgo técnico en decisiones financieras

Cyber Risk Quantification: cómo la metodología FAIR traduce vulnerabilidades, activos y amenazas en pérdida anual esperada (ALE) y Value at Risk — en euros, en el lenguaje del comité de auditoría.

CAPACIDAD	AUDIENCIA	EDICIÓN
Cyber Risk Quantification	CISO · Riesgo · CFO · Auditoría	2026

LECTURA	CLASIFICACIÓN	FUENTE
10 páginas	Público	Plataforma CSURFACE

RESUMEN EJECUTIVO

El riesgo que no tiene precio no tiene decisión

La tesis de este whitepaper, en una página — lo que el consejo necesita saber antes del detalle metodológico.

COSTO MEDIO DE UNA BRECHA

€3,90M

promedio en Brasil en 2025 (IBM Cost of a Data Breach)

SANCIÓN ADMINISTRATIVA RGPD

2%

de la facturación por infracción, limitada a €20M

TIEMPO PARA IDENTIFICAR Y CONTENER

241 días

promedio global en 2025 — el menor en nueve años (IBM)

Los programas de seguridad maduros producen datos en abundancia: número de CVEs abiertas, tiempo medio de remediación, cobertura de scans, postura de controles. Son indicadores útiles para la gestión operativa del SOC. Son, sin embargo, prácticamente **inútiles para el comité de auditoría, para el consejo y para el CFO** — que necesitan decidir presupuesto, reservas de capital y apetito de riesgo.

La causa raíz es una falla de lenguaje. La seguridad opera en CVE, CVSS y MTTR; el consejo opera en exposición, EBITDA y retorno sobre el capital. Sin un denominador común, la inversión en seguridad se aprueba sin criterio objetivo, la decisión de aceptar un riesgo no tiene trade-off explícito y la renovación del seguro cibernético se apoya en las premisas de peor caso del corredor — no en las premisas de la propia organización.

El **Cyber Risk Quantification (CRQ)** resuelve esa brecha. Aplicando la metodología FAIR — Factor Analysis of Information Risk —, el CRQ convierte la telemetría técnica en **exposición financiera medible**: pérdida anual esperada (ALE) y Value at Risk, expresados en euros. Esta es la métrica que el consejo aprueba, que la auditoría externa documenta y que el regulador espera ver.

La tesis. "Tenemos 47 vulnerabilidades críticas" es un dato sin unidad de decisión — no fundamenta aprobación de presupuesto, dimensionamiento de reservas ni definición de apetito de riesgo. "Nuestra exposición cibernética es de € 11 millones al año, con VaR P90 de € 20,5 millones" es una magnitud financiera que el consejo ya sabe evaluar y comparar con otras exposiciones del portafolio.

Lo que cubre este whitepaper

- Por qué los indicadores técnicos no sostienen decisiones de capital.
- Dónde se detienen los heat maps cualitativos y los scores externos de postura.
- La metodología FAIR aplicada al contexto regulatorio brasileño.
- El modelo cuantitativo de CSURFACE, con un ejemplo íntegramente calculado.

EL ESCENARIO · PARTE 01

Dos idiomas, una misma decisión

Por qué la seguridad y el consejo no se entienden — y lo que esa brecha le cuesta a la organización.

EL IDIOMA DE LA SEGURIDAD

Indicadores técnicos

CVEs abiertas · CVSS · MTTR · Cobertura de scans · Postura de controles

→

EL IDIOMA DEL CONSEJO · CRQ TRADUCE

Magnitudes financieras de decisión

Pérdida anual esperada (ALE) · Value at Risk · P90 / P99 · Exposición en euros · Apetito de riesgo · Reserva de capital · Costo-beneficio de remediación

El indicador técnico no llega a la mesa de decisión

El equipo de seguridad opera con indicadores técnicos — número de CVEs abiertas, tiempo medio de remediación, número de scans, porcentaje de cobertura. Son esenciales para la gestión del día a día. Pero no responden a las preguntas que definen el programa:

- El **comité de auditoría** necesita evaluar si el programa de seguridad es adecuado al riesgo del negocio.
- El **consejo** necesita aprobar un presupuesto de seguridad proporcional a la exposición real.
- El **CFO** necesita dimensionar reservas de capital para el riesgo cibernético.
- El **corredor de seguro cibernético** necesita cuantificar la exposición para tarifar la póliza.
- La **auditoría externa** evalúa el programa bajo frameworks como COSO ERM.

Ninguna de esas preguntas se responde con "tenemos 47 críticas". Todas se responden con un valor financiero.

Lo que produce la ausencia de cuantificación

1. **Subinversión crónica.** El consejo prioriza lo que entiende. Sin un valor financiero asociado al riesgo cibernético, el presupuesto de seguridad compite en desventaja con iniciativas que ya llegan cuantificadas.
2. **Decisiones de riesgo arbitrarias.** Sin cuantificación, aceptar o tratar un riesgo resulta de un juicio no documentado — sin el trade-off explícito entre el costo de la remediación y el costo esperado del incidente.
3. **Seguro cibernético mal tarifado.** Sin cuantificación propia, la empresa acepta la premisa de peor caso del corredor — y paga prima por una cobertura desalineada de la exposición real.

La brecha tiene un costo directo. El costo medio de una brecha de datos en Brasil llegó a **€3,90M** en 2025 (IBM Cost of a Data Breach 2025), y la sanción administrativa de la RGPD puede alcanzar el 2% de la facturación, limitada a €20M por infracción. Sin cuantificar esa exposición, la organización no dispone de criterio para evaluar si su nivel de inversión en seguridad es adecuado, insuficiente o excesivo — y cada una de esas desviaciones tiene consecuencias financieras distintas y medibles.

Por qué esto importa. El riesgo que no tiene precio no entra en el proceso de decisión de capital. Queda fuera del presupuesto, fuera del mapa de riesgos corporativos y fuera de la agenda del consejo — lo que significa que la organización no puede gestionarlo con la misma disciplina aplicada a los demás riesgos del negocio.

LIMITACIONES ACTUALES · PARTE 02

El heat map es opinión disfrazada de dato

Por qué las matrices cualitativas, los scores externos y el CVSS no sustituyen la cuantificación financiera.

Las matrices cualitativas 5×5 no sostienen decisiones

Las matrices de riesgo rojo-amarillo-verde son populares por ser simples. Esa simplicidad, sin embargo, esconde cuatro limitaciones estructurales:

ATENCIÓN **Ambigüedad**
¿"Probabilidad alta" significa 30% o 70%? La definición varía entre participantes, y la matriz no dispone de mecanismo para resolver esa divergencia.

ATENCIÓN **No permiten comparación**
Dos riesgos "altos" no son equivalentes — pero la matriz los trata como iguales.

CRÍTICO **No agregan**
Dos "altos" no suman de forma coherente a "muy alto". No hay aritmética detrás de los colores.

CRÍTICO **No conectan con el apetito de riesgo**
El consejo puede decir que no tolera una pérdida de € 100 millones. No puede decir que no tolera "rojo".

El punto. Un heat map comunica prioridad relativa entre riesgos ya conocidos. No comunica magnitud, no permite trade-off de capital y no dialoga con el apetito de riesgo del consejo. Para la mesa de decisión, es un punto de partida — nunca el destino.

Otros proxies — y dónde se detiene cada uno

Otros dos enfoques son comunes. Ambos tienen valor, y ambos tienen un límite claro.

1. **Scores externos de postura.** Notas de 0 a 1000 basadas en señales visibles — certificados, configuraciones, exposiciones — son útiles para benchmarking. Pero no se traducen en euros, ignoran la criticidad del activo y el contexto regulatorio, y no responden "¿cuánto invertir?".
2. **El CVSS como medida de riesgo.** El CVSS cuantifica severidad técnica teórica. Una nota 9.8 en una máquina de prueba sin datos no es el mismo riesgo que 9.8 en un servidor de producción con datos de tarjeta — y el CVSS, por sí solo, atribuye el mismo número a ambos.

Ninguno de estos instrumentos es prescindible — todos alimentan el modelo de cuantificación. El error es tratar a cualquiera de ellos como la respuesta financiera que el consejo espera.

EL ENFOQUE CSURFACE · PARTE 03

FAIR: descomponer el riesgo para poder calcularlo

El principio del FAIR y los datos que la plataforma usa para alimentar cada variable del modelo.

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 en dos factores.

→

2 Frecuencia de eventos de pérdida
Frecuencia de amenaza × Vulnerabilidad — la probabilidad anual de un evento material.

→

3 Magnitud de la pérdida
Pérdida primaria + Pérdida secundaria — el costo esperado por evento.

→

4 Distribución
Cada variable se convierte en un rango probabilístico para la simulación de Monte Carlo.

El principio: separar y cuantificar

El FAIR — Factor Analysis of Information Risk — es un estándar abierto que descompone el riesgo en variables observables, en vez de tratarlo como un todo opaco. La estructura es la del diagrama de arriba:

$$\text{Riesgo} = \text{Frecuencia de eventos de pérdida} \times \text{Magnitud de la pérdida}$$
$$\text{Frecuencia de eventos de pérdida} = \text{Frecuencia de amenaza} \times \text{Vulnerabilidad}$$
$$\text{Magnitud de la pérdida} = \text{Pérdida primaria} + \text{Pérdida secundaria}$$

Cada variable se estima como una **distribución de probabilidad** — lo que reconoce la incertidumbre inherente y permite la simulación de Monte Carlo. La pérdida primaria es el costo directo del incidente; la secundaria incluye multas, pérdida de clientes y daño de marca.

El FAIR no sustituye el juicio técnico — lo organiza. Cada estimación queda explícita, auditable y revisable.

Lo que alimenta el modelo

El CRQ de CSURFACE no requiere que la organización estime parámetros sin base empírica. El modelo se alimenta de los datos que la propia plataforma ya recolecta de forma continua:

- **Telemetría técnica.** Número de activos, vulnerabilidades y criticidad — en tiempo real, provenientes del descubrimiento continuo de la plataforma.
- **Telemetría de amenaza.** El *threat sensor* de CSURFACE va más allá de los scores estáticos de CVSS y de los índices de probabilidad de explotación y catálogos de explotación activa: observa actividad de amenazas, intentos de explotación, inteligencia de exploits e indicadores de campaña — señales en tiempo real que calibran la frecuencia de eventos en el modelo.
- **Contexto de negocio.** Sector, facturación y número de colaboradores, usados para calibrar probabilidad y magnitud con referencias de mercado.
- **Historial de incidentes.** Eventos de la propia organización, cuando existen, sumados a referencias sectoriales públicas.
- **Postura de controles.** Cobertura de logs, MFA, ciclo de patches y backups — factores que modulan la probabilidad.

La precisión del modelo crece proporcionalmente a la amplitud y a la actualidad de la telemetría recolectada. La calibración es continua y acompaña la telemetría a medida que evoluciona.

El modelo se alimenta de evidencia observada. Los activos, las vulnerabilidades y la criticidad que entran en el cálculo de riesgo provienen del descubrimiento continuo de la propia plataforma CSURFACE — la misma que, en 68 organizaciones, mapeó **122 mil activos externos** y, en 16 análisis detallados, **2.361 vulnerabilidades**. La cuantificación es tan sólida como el inventario que la sustenta.

EL ENFOQUE CSURFACE · PARTE 03

El modelo, parámetro por parámetro

Cómo se calculan probabilidad y magnitud, con los multiplicadores calibrados por el benchmark de 2025.

Probabilidad base sectorial

La probabilidad anual de un incidente material parte de una referencia por sector, ajustada por un multiplicador de madurez (Básica 1,4× · Intermedia 1,0× · Avanzada 0,65×).

SECTOR	P(INCIDENTE / AÑO)	SECTOR	P(INCIDENTE / AÑO)
Salud	34%	Telecom	26%
Financiero	32%	Educación	24%
Gobierno	30%	Industria	22%
Retail	28%	Energía	20%

Magnitud — la fórmula del SLE. La pérdida esperada por evento (Single Loss Expectancy) parte del costo medio nacional y se ajusta por sector, tamaño y tamaño de la superficie:

$$SLE = €3{,}90M \times \text{mult. sectorial} \times (\text{facturación} \div €\,200M)^{0,35} \times (\text{nº de activos} \div 500)^{0,25}$$

Los exponentes fraccionarios evitan la linealidad ingenua: duplicar la facturación no duplica la pérdida esperada.

Multiplicadores de costo por sector

Derivados de la razón entre el costo medio del sector y el promedio nacional del IBM Cost of a Data Breach 2025.

SECTOR	MULT.	SECTOR	MULT.
Salud	1,59×	Telecom	0,92×
Financiero	1,24×	Educación	0,78×
Servicios	1,18×	Retail	0,72×
Energía	1,00×	Gobierno	0,68×
Industria	0,95×	Otros	1,00×

Estimaciones CSURFACE a partir de las proporciones sectoriales del IBM 2025: Salud € 11,43M; Financiero € 8,92M; Servicios € 8,51M. Promedio nacional (IBM 2025): €3,90M.

De la pérdida por evento al número del consejo

- **ALE** = probabilidad ajustada × SLE — la pérdida anual esperada.
- **VaR P90** — el percentil 90 de la distribución de pérdidas, que supera el ALE y orienta decisiones de capital.
- **VaR P99** — la cola del 99%, que supera materialmente el ALE y sirve para reservas y cobertura de seguro.

APLICACIÓN · PARTE 04

Del inventario técnico al número en euros

Un cálculo completo, paso a paso: una minorista con € 1,2 mil millones de facturación.

PÉRDIDA ANUAL ESPERADA (ALE)

€ 11,1M

probabilidad ajustada × SLE

VALUE AT RISK · P90

€ 20,5M

el número para la decisión de capital

EXPOSICIÓN A MULTA RGPD

€ 17,5M

sanción potencial ponderada por la probabilidad

El escenario y el cálculo

Una minorista omnicanal, facturación de **€ 1,2 mil millones**, 4.500 colaboradores, **8.700 activos** descubiertos por la plataforma y madurez de seguridad intermedia. El modelo recorre cada parámetro:

- **Probabilidad.** Base del retail (28%), ajustada por madurez y por el tamaño de la superficie — probabilidad ajustada de aproximadamente **56%**.
- **SLE.** €3,90M × 0,72 (retail) × $(1.200 \div 200)^{0,35}$ × $(8.700 \div 500)^{0,25}$ ≈ **€ 19,8 millones**.
- **ALE.** 56% × € 19,8M ≈ **€ 11,1 millones** al año.
- **VaR P90 / P99.** Como estimación paramétrica de la cola, 1,85 × ALE ≈ **€ 20,5M**; 3,6 × ALE ≈ **€ 39,9 millones**.
- **Multa RGPD.** mín(€ 50M; facturación × 2%) × sensibilidad del retail (1,3) × probabilidad ≈ **€ 17,5 millones**.

El resultado, lado a lado

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

Valores calculados con el modelo recalibrado de CSURFACE, base IBM Cost of a Data Breach 2025.

El lenguaje del consejo. "Nuestra exposición cibernética anual es de € 11,1 millones, con VaR P90 de € 20,5 millones y exposición regulatoria de € 17,5 millones. Reducir el ALE en un 20% exige una inversión incremental cuya relación costo-beneficio es favorable." Esta es la formulación que permite al consejo deliberar con el mismo rigor aplicado a otros riesgos del portafolio.

EL ENFOQUE CSURFACE · PARTE 03

La exposición en euros es una métrica viva

Cómo el ALE acompaña cada cambio en el inventario y en la amenaza — y cómo el CRQ sustenta la documentación regulatoria.

EVALUACIÓN DE RIESGO TRADICIONAL

1x

por año — una foto estática que envejece al día siguiente de la entrega.

→

CRQ CLOSED-LOOP DE CSURFACE

24/7

el ALE acompaña cada cambio en el inventario, en la amenaza y en la remediación.

El loop cerrado en operación

El CRQ de CSURFACE es un cálculo vivo. Está integrado a las demás capacidades de la plataforma, y la exposición financiera se recalcula siempre que la realidad cambia:

1. **Una vulnerabilidad crítica es remediada.** La probabilidad ajustada cae y el ALE se recalcula automáticamente el mismo día.
2. **Un activo crítico es descubierto.** El descubrimiento continuo lo añade al alcance, el tamaño de la superficie sube y el SLE se reestima.
3. **El threat sensor detecta explotación activa de una CVE del inventario.** La explotación confirmada eleva la probabilidad, y la exposición se retarifica al alza.
4. **Una credencial corporativa se filtra.** El monitoreo de credenciales incorpora el impacto adicional al cálculo de magnitud.

Compatibilidad regulatoria

La cuantificación financiera es exactamente lo que reguladores y frameworks de gobernanza esperan. El CRQ apoya directamente:

- **BACEN.** Gestión integrada de riesgos con cuantificación financiera de la exposición cibernética.
- **CVM.** Deberes fiduciarios de administradores en la evaluación y divulgación de riesgos materiales.
- **RGPD / ANPD.** Informes de impacto a la protección de datos (RIPD) sustentados por datos cuantitativos.
- **ISO 27005 y COSO ERM.** Frameworks de gestión de riesgo plenamente compatibles con el enfoque FAIR.

De la auditoría a la decisión. Porque cada estimación del modelo es explícita y trazable, el CRQ produce una traza auditable: el comité de auditoría puede verificar el origen de cada parámetro, y el consejo recibe un digest mensual con la exposición actualizada — en vez de un informe anual con datos que ya no reflejan la realidad operativa.

APLICACIÓN Y RESULTADOS · PARTE 04

De la calculadora pública al módulo integrado

De la estimación sectorial al informe defendible: el recorrido de implementación y los entregables en cada etapa.

TIME-TO-VALUE · DE LA ESTIMACIÓN SECTORIAL AL INFORME DEFENDIBLE

1 **Día 1**
Estimación inmediata por la calculadora pública, sin datos internos.

→

2 **Semana 1**
El descubrimiento continuo alimenta el modelo con el inventario real de activos.

→

3 **Semana 2**
El threat sensor — explotación observada e inteligencia de exploits — calibra la probabilidad.

→

4 **Mes 1**
Primer informe ejecutivo de CRQ, listo para el comité de auditoría.

→

5 **Mes 3+**
Loop cerrado en régimen: el ALE fluctúa diariamente y genera un digest mensual.

Dos puntos de entrada

El CRQ ofrece dos modalidades de uso. La primera opera exclusivamente con parámetros sectoriales públicos:

- **La calculadora pública de riesgo.** Disponible en csurface.io, estima el ALE y el VaR del sector a partir de pocos parámetros — facturación, sector, número de colaboradores y activos. Es la puerta de entrada: una primera lectura de exposición en segundos, sin registro.
- **El módulo CRQ integrado.** La versión completa, dentro de la plataforma. Sustituye las estimaciones sectoriales por el inventario real de la organización, descubierto y clasificado de forma continua, y mantiene el loop cerrado de recálculo.

La calculadora da el orden de magnitud. El módulo integrado da el número defendible ante una auditoría.

Lo que entrega cada etapa

Calculadora pública — orden de magnitud
Una primera lectura de exposición en segundos, sin registro ni datos internos.

ATENCIÓN **Inventario real — sustituye la estimación**
El descubrimiento continuo cambia referencias sectoriales por el inventario descubierto y clasificado.

ATENCIÓN **Calibración por amenaza — probabilidad real**
El threat sensor ajusta la probabilidad por la explotación observada y por la inteligencia de exploits, sustituyendo scores estáticos por evidencia operativa.

CRÍTICO **Informe CRQ — número defendible**
ALE y VaR trazables, listos para la agenda del comité y para la auditoría externa.

Lo que cambia en la sala del consejo. El riesgo cibernético deja de ser un ítem técnico presentado una vez por año y pasa a ser una línea cuantificada del mapa de riesgos corporativos — comparable, agregable y directamente ligada al apetito de riesgo aprobado por el consejo.

PRÓXIMOS PASOS

La próxima reunión de riesgo puede comenzar con un número en euros

El Cyber Risk Quantification es una de las capacidades de la plataforma CSURFACE — una plataforma de Continuous Exposure Management. En una plataforma integrada, reúne descubrimiento continuo de la superficie externa con Machine Learning, análisis de la cadena digital de proveedores, validación activa de explotabilidad donde hay cobertura de pruebas, con monitoreo pasivo en el resto de la superficie, inteligencia de amenazas con priorización dinámica, monitoreo de credenciales filtradas y cuantificación financiera de riesgo. Opera de forma 100% externa — sin agente y sin instalación —, con integraciones opcionales de nube, WAF y CIEM para organizaciones que necesitan visibilidad profunda de esas capas.

Use la calculadora de riesgo

Estime el ALE y el VaR de su sector en segundos, sin registro — la puerta de entrada a la cuantificación financiera de riesgo.

Conozca el módulo CRQ

En una demostración, vea el análisis FAIR aplicado al inventario real de la organización, con el loop cerrado de recálculo continuo del ALE.

Lea el whitepaper de Threat Intelligence

Priorización dinámica de vulnerabilidades — uno de los insumos críticos para el cálculo de probabilidad del CRQ.

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

Recibir análisis preliminar gratuito