# LABORATORIO COLABORATIVO DE TÉCNICAS DE EVALUACIÓN DEL RIESGO APLICADAS A ESCENARIOS DE CIBERSEGURIDAD Y CIBERDEFENSA

**INTEGRANTES:** Carolina Salinas – Laura Gutiérrez – Johan Tamara – Natalia Forero – Ayda Castro.

Escuela Superior de Guerra “General Rafael Reyes Prieto”

MAECI / GESTIÓN DE RIESGOS CIBERNÉTICOS
Enero, 2026.

# LABORATORIO COLABORATIVO DE TÉCNICAS DE EVALUACIÓN DEL RIESGO APLICADAS A ESCENARIOS DE CIBERSEGURIDAD Y CIBERDEFENSA

| Técnica | Objetivo de la técnica | Tipo de incertidumbre que aborda | Nivel de complejidad | Ventajas | Limitaciones | Requisitos de información | Nivel de madurez organizacional requerido | Aplicabilidad en ciberseguridad / ciberdefensa |
|---|---|---|---|---|---|---|---|---|
| **Indices de Riesgo** | Crear un puntaje numérico compuesto para comparar riesgos de un mismo sistema. | Incertidumbre por múltiples factores que influyen en el riesgo (ej.: exposición, controles, criticidad). | Media: fácil de usar, pero exige diseñar fórmula/escala y validar. | *Puntaje sencillo para jerarquizar riesgos.<br>*Integra múltiples factores en un solo número. | * Si el modelo no está validado, puede no tener sentido.<br>* Puede “parecer exacto” y usarse mal (ej.: costo/beneficio).<br>* A veces no hay modelo sólido para combinar factores poca confiabilidad. | * Requiere análisis del sistema, comprender fuentes de riesgo y cómo surgen consecuencias.<br>* También se apoya en datos históricos para validar. | Media–Alta: necesitas gobernanza para definir factores, pesos, validación y evitar “falsa precisión”. | Excelente para priorizar riesgos tipo: criticidad de activos, debilidades, exposición, impacto operacional, etc. |
| **Matriz de Consecuencias / Posibilidades** | Visualizar riesgos según consecuencia y posibilidad, y asignar una “importancia” del riesgo. | Incertidumbre por estimación cualitativa/ordinal de consecuencia y posibilidad, depende del juicio experto y datos disponibles. | Baja–Media: es fácil de usar, pero diseñar escalas sólidas requiere experiencia. | *Fácil y rápida jerarquización.<br>*Visualización clara del riesgo por consecuencia/posibilidad.<br>*Permite comparar riesgos con distintos tipos de consecuencia. | * Muy subjetiva: diferentes personas califican distinto el mismo riesgo.<br>* Difícil definir escalas sin ambigüedad y que sean consistentes.<br>* No se pueden “sumar riesgos” directamente. | * Se debe construir una matriz adaptada al contexto y contar con datos para escalas realistas.<br>* Requiere equipo con conocimiento del riesgo y datos de apoyo. | Media: puedes iniciar rápido, pero se recomienda calibración, consistencia y criterio común. | Muy útil para SOC / CISO: priorizar incidentes, vulnerabilidades, amenazas; ideal para comunicar a directivos por su visualización. |
| **Analisis de Corbatin** | Visualizar y analizar cómo un evento peligroso puede ocurrir, identificar causas, consecuencias y barreras preventivas y mitigadoras, y evaluar la criticidad del riesgo. | Epistémica y aleatoria de forma moderada: incertidumbre sobre causas/consecuencias y desempeño de barreras. | Medio (requiere modelado lógico y conocimiento del proceso). | Representación visual clara del riesgo - Integra causas, consecuencias y controles - Facilita comunicación con stakeholders - Permite priorizar barreras críticas | Puede simplificar relaciones complejas - Depende del juicio experto - No incluye cálculos probabilísticos avanzados | * Descripción del proceso o sistema.<br>* Identificación del evento peligroso.<br>* Información sobre causas, consecuencias y controles existentes.<br>* Datos operacionales básicos o juicio experto. | Intermedio: capacidad para discutir riesgos, documentar procesos y evaluar controles. | Alta, útil para: - Análisis de eventos ciber (cyber bowtie) - Ataques de APT y ransomware (identificar causas y barreras) - Evaluación de medidas de defensa en C2/C5ISR - Gestión de controles preventivos/detectivos/mitigadores En ciberdefensa permite visualizar vectores de ataque, barreras y consecuencias. |
| **Curvas en S** | Visualizar la relación entre las consecuencias y su posibilidad, graficada como una función de distribución acumulativa. | La técnica aborda la incertidumbre variable y epistemológica al considerar la variabilidad de los parámetros y apoyarse en juicios expertos para estimar valores mínimos, probables y máximos cuando los datos son insuficientes. | Media: Organizaciones que ya han superado matrices simples de probabilidad x impacto. | * La técnica permite representar la magnitud del riesgo cuando las consecuencias se distribuyen en un rango de valores.<br>* Se basa en juicios expertos para estimar impactos mínimo, probable y máximo, transformándolos en una distribución acumulada comprensible, cuya precisión mejora con la disponibilidad de datos fiables. | * El método puede transmitir una sensación de precisión superior a la que realmente permiten los datos disponibles.<br>* La representación de distribuciones mediante valores puntuales implica supuestos e incertidumbres sobre la forma de la distribución y la validez de las estimaciones.<br>* Las distribuciones basadas en datos históricos aportan información limitada sobre eventos futuros de baja probabilidad y consecuencias extremas. | La Curva en S se construye a partir de datos o juicios expertos, y su validez aumenta a medida que se dispone de mayor cantidad de datos fiables. | Moderado / Alto: Requiere un nivel con criterios de impacto definidos, juicio experto confiable y capacidad de comunicar estimaciones sin interpretarlas como predicciones. | En ciberseguridad, permiten representar impactos variables de incidentes como ransomware o indisponibilidad del servicio, considerando tiempos de detección, respuesta y recuperación como un conjunto acumulado de consecuencias. |

# Análisis Bow-Tie

**Compromiso de sistemas críticos que soportan la operación esencial de la infraestructura**, generando indisponibilidad del servicio y pérdida de control operacional.

| | |
|---|---|
| Impacto legal / regulatorio | - Incumplimiento de normas sectoriales (continuidad, seguridad de la información)<br>- Investigaciones por entes reguladores<br>- Sanciones administrativas<br>- Demandas de clientes o terceros |
| Impacto reputacional | - Pérdida de confianza de clientes y aliados<br>- Cobertura negativa en medios<br>- Deterioro de la imagen corporativa<br>- Afectación al valor de marca y percepción de resiliencia |
| Controles preventivos (antes del evento) | - Autenticación multifactor (MFA) obligatoria<br>- Segmentación estricta de redes IT/OT<br>- Gestión de vulnerabilidades continua<br>- Concienciación avanzada contra phishing<br>- Hardening y control de accesos privilegiados |
| Controles mitigantes (después del evento) | - Plan de respuesta a incidentes (CSIRT/SOC)<br>- Backups inmutables y pruebas de restauración<br>- Aislamiento rápido de sistemas comprometidos<br>- Plan de Continuidad del Negocio (PCN)<br>- Gestión de crisis y comunicación externa |

# Análisis Bow-Tie

## Aspectos clave

- **Visualizar claramente cómo un ciberataque escala** desde amenazas técnicas hasta impactos de negocio.
- Evidenciar que **los mayores daños no siempre provienen del ataque inicial**, sino de **fallas en controles preventivos y tiempos de reacción.**
- Demostrar que la **resiliencia organizacional** depende del equilibrio entre:
  - Controles **preventivos** (evitar que ocurra)
  - Controles **mitigantes** (reducir el daño cuando ocurre)
- En infraestructura crítica, este enfoque es clave para **justificar inversiones en ciberseguridad**, fortalecer la **defensa en profundidad** y mejorar la **capacidad de respuesta estratégica.**

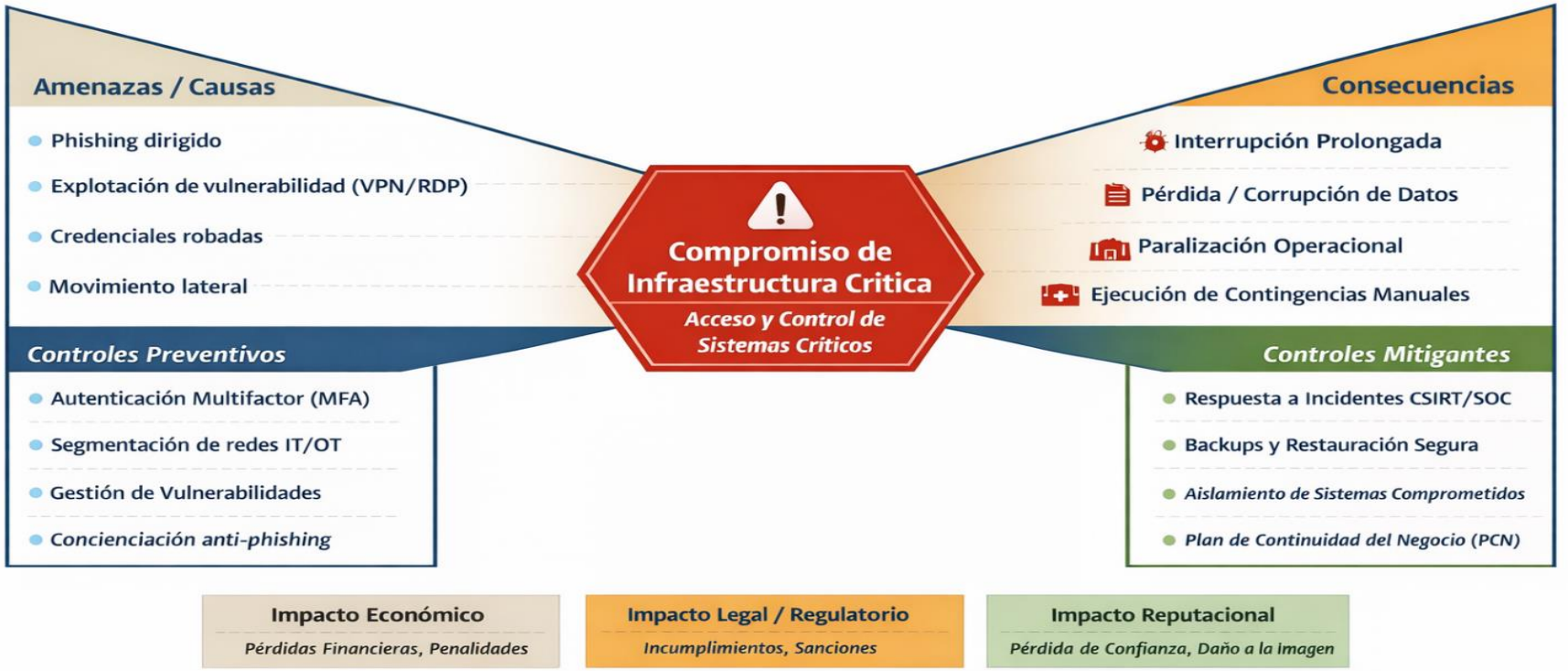
# Análisis Bow-Tie

## Conclusión

- La aplicación de la técnica de **Corbatín** a un escenario realista de ciberataque evidencia que los riesgos tecnológicos se transforman rápidamente en **riesgos económicos, legales y reputacionales**. Su valor principal está en **conectar la ciberseguridad con el impacto real en el negocio**, facilitando decisiones informadas a nivel de **alta dirección, comités de riesgo y autoridades regulatorias**.

# Análisis Bow-Tie

Diagrama



# Análisis Curvas S

En este escenario se analiza un **ataque DDoS** dirigido contra la **red transaccional de una entidad bancaria**, cuyo objetivo principal es **interrumpir la disponibilidad de los servicios financieros** ofrecidos a los clientes.

| Supuesto Base del Ataque | Consecuencias |
|---|---|
| Se asume un ataque de tipo DDoS mixto, combinando:<br>Ataques volumétricos, orientados a saturar el ancho de banda.<br>Ataques a nivel de aplicación, dirigidos a los servicios críticos del banco. | Como consecuencia, se produce una indisponibilidad total de los canales de atención y operación.<br>Es importante resaltar que no existe exfiltración de información; el impacto del evento es estrictamente operativo, no asociado a la pérdida de confidencialidad de los datos. |
| **Base del Ataque** | |
| Tipo de ataque: DDoS volumétrico + aplicación<br>Impacto: Indisponibilidad total de canales<br>Core bancario<br>Canales digitales (app, web)<br>Cajeros automáticos<br>Pagos y transferencias | |

# Análisis Curvas S

En este escenario se analiza un **ataque DDoS** dirigido contra la **red transaccional de una entidad bancaria**, cuyo objetivo principal es **interrumpir la disponibilidad de los servicios financieros** ofrecidos a los clientes.

| ESCENARIOS CRISIS FINANCIERA | | |
|---|---|---|
| ESCENARIO 1 – CRISIS BAJA<br>Duración del ataque - 2 a 7 horas<br>Impacto operativo<br>Ventana corta<br>Pico de congestión en horas laborales<br>Recuperación el mismo día | ESCENARIO 2 – CRISIS MEDIA<br>Duración del ataque - 7 a 24 horas<br>Impacto operativo<br>Día completo sin operación<br>Caída en comercios y pagos<br>Clientes corporativos afectados<br>Interrupción de pagos críticos (nómina, proveedores) | ESCENARIO 3 – CRISIS ALTA<br>Duración del ataque - 24 – 72 horas o más<br>Impacto operativo<br>Paralización total del banco<br>Incumplimiento de SLA críticos<br>Riesgo sistémico (interbancario)<br>Activación de planes de continuidad externos |

# Análisis Curvas S

| ESCENARIO 1 – CRISIS BAJA | | ESCENARIO 2 – CRISIS MEDIA | | ESCENARIO 3 – CRISIS ALTA | |
|---|---|---|---|---|---|
| Concepto | Estimación | Concepto | Estimación | Concepto | Estimación |
| | | | | Transacciones no realizadas | USD 400 – 700 millones |
| | | Transacciones no realizadas | USD 150 – 250 millones | Ingresos por comisiones perdidos | USD 1.5 – 2.5 millones |
| Transacciones no realizadas | USD 20 – 35 millones | Ingresos por comisiones perdidos | USD 600.000 – 1.4 millones | Demandas colectivas y conciliaciones | USD 2.5 – 6 millones |
| Ingresos por comisiones perdidos | USD 120.000 – 1.4 millones | Penalizaciones contractuales (empresas) | USD 900.000 – 1.1 millones | Multas regulatorias | USD 1 – 2 millones |
| Costos de mitigación (CDN, scrubbing, SOC) | USD 50.000 – 300.000 | Costos técnicos y refuerzo infraestructura | USD 250.000 – 400.000 | Costos de reputación (campañas, compensaciones) | USD 1.5 – 2.8 millones |
| Pérdida financiera directa | USD 250.000 – 1.8 millones | Pérdida financiera directa | USD 1,8 – 2,8 millones | Pérdida financiera total estimada | USD 2.9 – 3.5+ millones |

# Análisis Curvas S

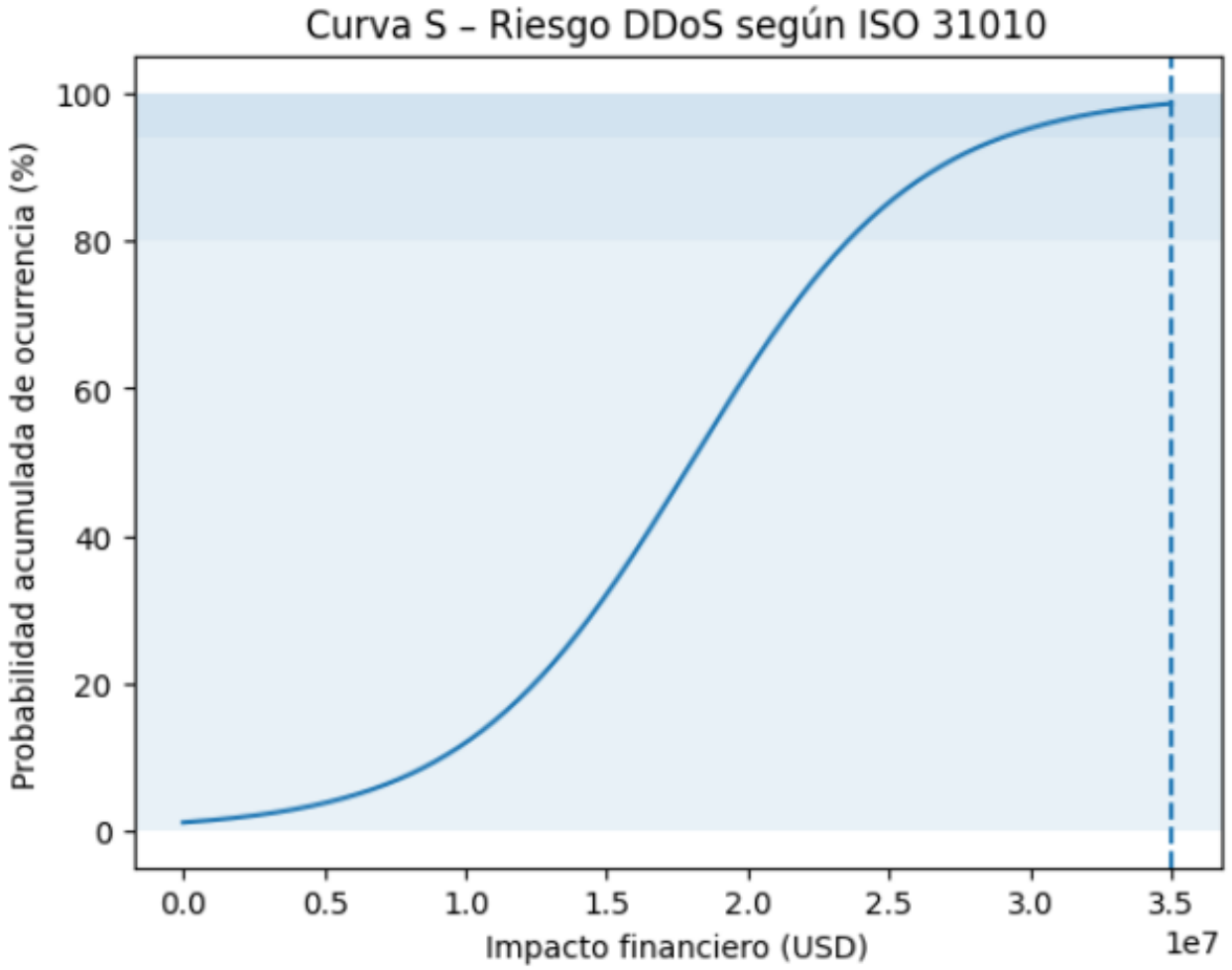
| ESCENARIOS CRISIS FINANCIERA | | |
|---|---|---|
| **ESCENARIO 1 – CRISIS BAJA** | **ESCENARIO 2 – CRISIS MEDIA** | **ESCENARIO 3 – CRISIS ALTA** |
| Impacto reputacional<br>Bajo<br>Reclamos en redes sociales<br>Comunicaciones de contingencia suficientes | Impacto reputacional<br>Medio<br>Medios de comunicación nacionales<br>Caída temporal de confianza<br>Downtime reportado públicamente | Impacto reputacional<br>Severo<br>Riesgo de “bank run” digital<br>Pérdida de calificación de confianza<br>Impacto en valor de marca y acciones (si aplica) |
| Pérdida de clientes<br>< 0,1% (clientes altamente sensibles)<br>Principalmente clientes digitales jóvenes | Pérdida de clientes<br>0,5% – 1%<br>Migración a fintechs y bancos digitales<br>Riesgo alto en clientes empresariales | Pérdida de clientes<br>3% – 7%<br>Alta fuga de clientes premium y corporativos<br>Reducción sostenida de ingresos futuros |

# Análisis Curvas S

| ESCENARIOS CRISIS FINANCIERA | | |
|---|---|---|
| **ESCENARIO 1 – CRISIS BAJA** | **ESCENARIO 2 – CRISIS MEDIA** | **ESCENARIO 3 – CRISIS ALTA** |
| Riesgo legal / regulatorio<br>No hay sanción<br>Reporte informativo al regulador<br>Sin demandas colectivas | Riesgo legal / regulatorio<br>Investigación del regulador<br>Posibles multas leves<br>Exigencia de plan de mejora<br>Demandas individuales (cuantía moderada) | Riesgo legal / regulatorio<br>Sanción grave del regulador<br>Auditoría forense obligatoria<br>Riesgo de intervención o vigilancia especial<br>Demandas colectivas de alto valor |
| Conclusión financiera: Evento absorbible por provisiones operativas. | Conclusión financiera: Impacto material en resultados trimestrales. | Conclusión financiera: Evento potencialmente existencial, afecta solvencia y proyección del negocio. |

# Análisis Curvas S

| ESCENARIOS CRISIS FINANCIERA |
| --- |
| ESCENARIO 1 – CRISIS BAJA<br>2 - 7 h / USD 0,25 – 1,8 M<br>Probabilidad = 99% - 45% |
| ESCENARIO 2 – CRISIS MEDIA<br>7 – 24 h / USD 1,8 M – 2,8 M<br>Probabilidad = 44% - 8% |
| ESCENARIO 3 – CRISIS ALTA<br>25 – 72 h / USD 2,9 M – 3,5+ M<br>Probabilidad = 7% - 1% |



# LECCIONES APRENDIDAS

| Dimensión | Síntesis para presentación académica |
|---|---|
| ¿Qué funcionó? | Permitió visualizar claramente la relación causa–evento–consecuencia, evidenciar el rol de los controles preventivos y mitigantes, y traducir riesgos técnicos a impactos de negocio comprensibles para tomadores de decisión. |
| ¿Qué no funcionó? | No cuantifica el riesgo por sí sola, depende del conocimiento del equipo y puede simplificar en exceso escenarios complejos si no se complementa con otras técnicas. |
| ¿Cuándo no usarla? | No es adecuada como técnica principal cuando se requiere análisis cuantitativo, escenarios altamente dinámicos o análisis técnico profundo de fallas. |
| Recomendaciones prácticas | Usarla como herramienta de comunicación estratégica, construirla desde eventos de negocio, validar controles con evidencia, complementarla con otras técnicas ISO 31010 y actualizarla tras incidentes reales. |
| Valor académico y profesional | Facilita el entendimiento integral del riesgo, fortalece la resiliencia organizacional y conecta la ciberseguridad con impactos económicos, legales y reputacionales. |