Telefónica Tech

CASO PRÁCTICO

Cuantificación del Ciberriesgo

Ataque de ransomware en una entidad financiera

Estevenson Solano
Senior GRC Consultant en Govertis, part of Telefónica Tech

telefonicatech.com

Índex

PREÁMBULO

Este caso práctico presenta un escenario hipotético de ciberataque tipo ransomware a una entidad financiera con el objetivo de ilustrar la aplicación de metodologías de análisis y cuantificación del ciberriesgo en un contexto realista. A través de este ejercicio, se integran marcos reconocidos como ISO 27005, NIST 800-30 y el modelo FAIR para estimar la pérdida financiera potencial, definir estrategias de mitigación y evaluar el retorno de inversión (ROI) en ciberseguridad.

El análisis incluye el uso de herramientas avanzadas como simulación Monte Carlo y análisis bayesiano, aportando una visión basada en datos para la toma de decisiones informadas por parte de la alta dirección y los órganos de gobierno corporativo. Este enfoque permite priorizar inversiones, alinear la estrategia de ciberseguridad con los objetivos de negocio y fortalecer la resiliencia frente a nuevos riesgos y ciberamenazas.

INTRODUCCIÓN

En este ejercicio se analiza un incidente simulado de ransomware que afecta a una institución financiera, centrado específicamente en el impacto sobre sus servicios de banca online. El objetivo es aplicar un enfoque integrado de gestión y cuantificación del ciberriesgo que permita:

- Identificar las amenazas, vulnerabilidades e impactos asociados al ataque.
- Cuantificar el riesgo mediante el modelo FAIR, estimando la frecuencia y magnitud de las pérdidas
- Evaluar opciones de tratamiento del riesgo, como la mitigación o la transferencia mediante ciberseguro.
- Justificar las decisiones de inversión en ciberseguridad a partir del análisis de retorno (ROI).
- Integrar los resultados en procesos de gobierno corporativo y toma de decisiones estratégicas.

Para ello se combinan los marcos metodológicos ISO 27005 y NIST 800-30 como referencia para la gestión cualitativa del riesgo, con FAIR para su cuantificación financiera, complementado con técnicas de análisis como la simulación Monte Carlo y el enfoque bayesiano.

Este caso práctico tiene un carácter ilustrativo y didáctico, y busca proporcionar un modelo replicable para la evaluación avanzada de ciberriesgos en entornos críticos y altamente regulados como el financiero.

Identificar los componentes de riesgos teniendo en cuenta los enfoques existentes de ISO 27005 y NIST 800-30 para identificar amenazas, vulnerabilidades e impactos.

Fuente de amenaza

Grupos organizados de ransomware dirigidos a servicios financieros.

Evento de la amenaza

Grupos organizados de ransomware dirigidos a servicios financieros.

Vulnerabilidad

Sistema de copia de seguridad obsoleto y falta de segmentación adecuada en la infraestructura y arquitectura tecnológica.

Impacto:

- Interrupción del negocio producto a la caída del sistema.
- Pérdidas financieras por el pago del rescate **si se paga.**
- Costes de recuperación de datos e investigación forense.
- Posibles multas o sanciones legales y regulatorias **GDPR, NIS2, DORA, SEC.**
- Pérdida de clientes por daños a la reputación.
- Pérdida económica y financiera de alto impacto.

Cuantificar el ciberriesgo mediante el modelo FAIR

Identificación de factores claves

- **Loss Event Frequency (LEF):** Frecuencia con la que se espera que ocurra este tipo de evento en un año.
- **Threat Event Frequency (TEF):** La probabilidad de que se produzca el ciberataque.
- **Vulnerability (Vuln):** La probabilidad de que los controles y las capacidades de ciberdefensa fallen.
- **Loss Magnitude (LM):** El impacto financiero del evento dividido en perdidas primarias directas y secundarias indirectas.

Estimación de Componentes FAIR

Estimación de la Frecuencia de Eventos de Pérdida (LEF)

Threat Event Frequency (TEF)

- Basado en inteligencia sobre amenazas, **instituciones financieras similares se enfrentan a intentos de ransomware cada 2 meses.**
- **Estimación del TEF: 6 ciberataques al año.**

Vulnerability (Vuln) – Probabilidad de que un ciberataque tenga éxito

- **Los controles existentes de seguridad (copias de seguridad, segmentación y endpoint) reducen la probabilidad de éxito.**
- La evaluación de seguridad indica un **40% de probabilidad de fallo de los controles de ciberseguridad por el ciberataque.**
- **Vulnerability: 0,40**

Loss Event Frequency (LEF) Calculation

- **LEF = TEF × Vulnerability.**
- **LEF = 6 × 0,40 = 2,4 eventos de ransomware al año.**

Estimación de la magnitud de la pérdida (LM)

La estimación de las magnitudes de las pérdidas incluye las pérdidas primarias **impacto directo** y las pérdidas secundarias **consecuencias indirectas como multas o sanciones legales y regulatorias, daños a la reputación, etc.**

Pérdida primaria (pérdidas financieras directas)	
Categoría de pérdida	**Coste estimado (USD)**
Caída del sistema (2 días)	2.000.000
Pago del rescate (si se paga)	1.500.000
Recuperación de datos y análisis forense	800.000
Compensación al cliente	500.000
Pérdida primaria Total	4.800.000
Pérdidas secundarias (impacto en la reputación y la normativa)	
Categoría de pérdida	**Coste estimado (USD)**
Multas reglamentarias (GDPR, SEC, etc.)	2.000.000
Fuga de clientes y pérdida de ingresos	3.500.000
Aumento de las inversiones en ciberseguridad	1.500.000
Total de pérdidas secundarias	7.000.000

- **Total Loss Magnitude (LM) = Perdida Primaria + Pérdida Secundaria**
- **LM = 4.800.000 + 7.000.000 = 11.800.000**

Cálculo de Expectativa de Perdida Anualizada (ALE)

- **ALE = LEF × LM**
- **ALE = 2,4 × 11.800.000**
- **ALE = 28.320.000 por años**

Interpretación y tratamiento del riesgo integrando ISO 27005 y NIST 800-30 para determinar cómo mitigar, transferir, aceptar o evitar el riesgo.

Opciones de tratamiento del ciberriesgo

1. Mitigación del riesgo: reducir la probabilidad o el impacto

- Implementar copias de seguridad inmutables protegidas air-gapped, con una inversión de 1 millón de dólares.
- Mejorar la segmentación de los sistemas bancarios críticos, con una inversión de 1,5 millones de dólares.
- Mejorar las tecnologías y herramientas de detección y respuesta al ransomware, con una inversión de 500.000 dólares.
- **Reducción estimada del riesgo:** 60% la vulnerabilidad baja de 0,40 a 0,16.

2. Transferencia del riesgo: estrategia de ciberseguro

- Cobertura del ciberseguro con una póliza de 10 millones de dólares, que cubre el tiempo o periodo de inactividad, los costes de recuperación y los honorarios legales.
- Prima anual: 2 millones de dólares.

3. Análisis de riesgo residual

Después de la mitigación, reevaluar y recalcular la vulnerabilidad.

- **Nuevo LEF = 6 × 0,16 = 0,96 (reducido de 2,4 eventos/año)**
- **Nuevo ALE = 0,96 × 11.800.000 = 11.328.000 (reducido de 28,3 millones de dólares /año).**
- **Reducción del riesgo = 60%.**

4. Toma de decisiones y justificación empresarial a C- suite y gobierno corporativo

- **Inversión necesaria (medidas de mitigación) = 3 millones de dólares.**
- **Reducción esperada de pérdidas anuales = 28,3 millones - 11, 3 millones = 17 millones de dólares.**

- **ROI = (Ahorro - Inversión) / Inversión.**
- **ROI = (17 millones - 3 millones) / 3 millones de dólares = 466%.**

Justificación del ciberseguro

- Póliza del ciberseguro (10 millones de dólares de cobertura) reduce la exposición financiera.
- Después del ciberseguro, la perdida máxima anual de bolsillo es de 1,3 millones de dólares en lugar de 11,3 millones de dólares.

Recomendación

- Invertir 3 millones de dólares en mejoras de ciberseguridad; **copias de seguridad, segmentación y endpoint.**
- Adquirir una póliza de ciberseguro de10 millones de dólares para cubrir el riesgo residual.
- Monitorizar y mejorar anualmente los modelados de riesgos usando la metodología NIST y ajustar las entradas de cuantificación de riesgo.
- Mantener informado a los órganos de gobierno corporativo y C-level (CEO, CFO, CISO, etc.) de las métricas de ciberriesgo para alinearlas con la estrategia empresarial y el cumplimiento normativo.

Valoración

Con este análisis de cuantificación de aproximación basado en FAIR, integrando principios de la ISO 27005 y NIST 800-30, proporciona un enfoque basado en datos para la toma de decisiones sobre ciberriesgos, al tiempo que se permite:

- Priorizar las inversiones de ciberseguridad en función del impacto financiero.
- Reducir la ciberexposición a través de controles y capacidades de ciberdefensa específicas.
- Aprovechar los ciberseguros como mecanismo de trasferencia de riesgo y agilidad.
- Alinear las estrategias cibernéticas con los objetivos empresariales y las exigencias regulatorias.

Anexo

Análisis tenidos en consideración:

Métricas de cuantificación adicionales

Tiempo medio de detección (MTTD) y el Tiempo medio de respuesta (MTTR) son esenciales para medir la eficacia de las capacidades de detección y respuesta a ciberincidentes.

Actual MTTD

- Media del sector para ciberataques de ransomware: 24 horas
- Con SIEM y mejoras en la inteligencia sobre amenazas: 6 horas
- MTTD antes de la inversión: 24 horas
- MTTD después de la inversión: 6 horas

Actual MTTR

- Incluye el tiempo para aislar los sistemas afectados, investigar y ejecutar los planes de respuesta.
- Sin detección y respuesta avanzada: 36 horas
- Con SOC mejorado y repuesta automatizada: 12 horas
- MTTR antes de la inversión: 36 horas
- MTTR después de la inversión: 12 horas

Impacto en la reducción de riesgos, ya que una detección y respuesta más rápida pueden reducir la magnitud de las perdidas al minimizar el tiempo de inactividad operativa y la exposición de los datos.

Retorno de la inversión en ciberseguridad (ROI)

El ROI de la ciberseguridad se calcula mediante la fórmula:

$$ROI = \frac{\textbf{Annual Loss Reduction} - \textbf{Investment Cost}}{\textbf{Investments Cost}} \times 100\%$$

- Inversión en nuevos controles de ciberseguridad (copias de seguridad, segmentación, endpoint), 3 millones de dólares.
- Reducción anual de perdidas (a partir del cálculo del CRQ): 17 millones de dólares.

Cálculo de ROI cibernético:

$$ROI = \frac{17\ \text{M} - 3\ \text{M}}{3\ \text{M}} \times 100\% = 466\%$$

Este ROI del 466% nos indica que la inversión en ciberseguridad está muy justificada y proporciona importantes beneficios financieros.

Impacto en la reducción de riesgos: Donde una detección y respuesta más rápidas pueden reducir la magnitud de las pérdidas al minimizar el tiempo de inactividad operativa y la exposición de los datos.

Objetivo de Punto de Recuperación (RPO)

Teniendo en cuenta que es el periodo máximo tolerable en el que puede producirse una pérdida de datos.

- **RPO actual:** 24 horas (copias de seguridad diarias).
- **Después de la inversión (copias de seguridad en la nube e inmutables):** 1 hora.

Al reducir el RPO se minimiza la pérdida de datos, lo que es crítico para las transacciones financieras.

Objetivo de tiempo de recuperación (RTO)

Teniendo en cuenta que es el tiempo máximo que los sistemas informáticos pueden estar inactivos antes de causar daños inaceptables.

- **RTO actual:** 48 horas (recuperación manual y copias de seguridad obsoletas).
- **Después de la inversión (conmutación por error automatizada y mejoras de plan de recuperación):** 8 horas.

Aquí un RTO más bajo garantiza que las operaciones de negocio se reanuden más rápidamente, reduciendo el impacto financiero y reputacional.

Tiempo de recuperación del trabajo (WRT)

Teniendo en cuenta que es el tiempo adicional necesario después de restaurar los sistemas de TI para reanudar completamente las operaciones de negocio.

- **WRT actual:** 12 horas (procesos de verificación manuales).
- **WRT optimizado:** 4 horas (validación automatizada y procedimientos de recuperación probados previamente).

Tiempo de inactividad máximo tolerable (MTD)

Teniendo en cuenta que es el tiempo máximo total de inactividad que una empresa puede soportar antes de que se produzcan daños irreversibles.

- El análisis de riesgos de negocio indica que el sistema de banca en línea tiene un tiempo máximo de inactividad tolerable de 72 horas.
- Proceso de recuperación actual (RTO + WRT): 60 horas.
- Proceso optimizado (RTO + WRT): 12 horas, muy por debajo del umbral MTD.

Hay que destacar que se confirma que las mejoras en RTO y WRT se ajustan a los objetivos de continuidad de negocio que incluyen las métricas de cuantificación del ciberriesgo, podemos ver su influencia.

Variable	Influencia	Impacto
MTTD y MTTR más cortos	Contención de amenazas más rápida	Menor exposición al ciberriesgo
Menor RPO	Minimiza la pérdida de datos	Reduce el impacto financiero y operativo
Menor RTO & WRT	Recuperación más rápida del sistema	Reduce los costes de interrupción del negocio
Alineación MTD	Garantiza la resiliencia	Previene el fracaso catastrófico del negocio
Alto ROI cibernético	Justifica la inversión en ciberseguridad	Mejora la toma de decisiones

Enfoque de modelización financiera

1. Simulación Monte Carlo para la estimación de pérdidas

A través de las simulaciones Monte Carlo busco modelar el impacto financiero teniendo en cuenta diversos factores de riesgo, como el tiempo de inactividad, la pérdida de datos, las sanciones reglamentarias y los daños a la reputación.

Supuestos y variables de entrada:

- **Tiempo de inactividad operativa:** estimado entre 12 y 72 horas (distribución triangular, Modo = 24 horas).
- **Multas reglamentarias (GDPR, NIS2, DORA, SEC):** Entre 5 y 50 millones de dólares (distribución normal, media = 25 millones de dólares, DE = 10 millones de dólares).
- **Probabilidad de pago de rescate:** 30% de probabilidad de pago, con peticiones de rescate entre 2 y 10 millones de dólares (distribución uniforme).

- **Ingresos comerciales perdidos por hora:** entre 1 y 5 millones de dólares (distribución logarítmica normal, media = 2,5 millones de dólares).
- **Costes de respuesta y recuperación de incidentes:** entre 3 y 15 millones de dólares (distribución exponencial, media = 7 millones de dólares).

Al aplicar las 10.000 iteraciones de Monte Carlo, la pérdida financiera esperada oscila entre 20 y 150 millones de dólares, con un intervalo de confianza del 95% de 45 a 85 millones de dólares.

2. Análisis bayesiano para la actualización de la probabilidad de riesgo

Dados los datos previos del incidente, la inferencia bayesiana actualiza la probabilidad de que vuelva a producirse el ransomware:

Probabilidad a priori:

- **Frecuencia histórica de ransomware en instituciones financieras:** 10% anual

Entrada de nuevos datos:

- **Aumento de los ataques en todo el sector** (+20% interanual).
- Información específica sobre amenazas que indica que los grupos de ransomware se dirigen a ellos

Aplicación de la actualización bayesiana:

$$P(A|B) = \frac{\mathbf{P}\,(\mathbf{B}|\mathbf{A}) \cdot \mathbf{P}\,(\mathbf{A})}{P(B)}$$

- **Probabilidad actualizada de ransomware:** 16% anual
- Expectativa de pérdida anualizada ajustada (ALE):

$$ALE = SLE\ x\ ARO$$

Donde SLE (Single Loss Expectancy) = 65 M de dólares (de Monte Carlo)

ARO (tasa anual de ocurrencia) = 0,16

ALE actualizada = 10,4 millones al año

3. Indicadores clave de rendimiento (KPI)

Metric	Pre-Investment	Post-Investment (With Cybersecurity Enhancements)
Mean Time to Detect (MTTD)	24 hours	6 hours
Mean Time to Respond (MTTR)	36 hours	12 hours
Recovery Point Objective (RPO)	24 hours	1 hour
Recovery Time Objective (RTO)	48 hours	8 hours
Work Recovery Time (WRT)	12 hours	4 hours

4. Tratamiento del riesgo y análisis coste-beneficio

Para mitigar los riesgos del ransomware, la institución financiera considera las siguientes estrategias:

Mitigation Strategy	Implementation Cost	Estimated Loss Reduction	Cyber ROI
AI-based Threat Detection	$3M	$17M	466%
Immutable Backups	$5M	$25M	400%
SOC Expansion	$10M	$35M	250%

Justificación:

Invertir 18 millones de dólares en mejoras combinadas de ciberseguridad da como resultado una reducción de pérdidas esperada de 77 millones de dólares, lo que demuestra un alto ROI y resiliencia estratégica.

Implicaciones estratégicas e integración de ERM

Al integrar el análisis de Monte Carlo y Bayesiano en su marco de Gestión de Riesgos Empresariales (ERM),

- Alinea el riesgo cibernético con los riesgos financieros, de crédito y de liquidez.
- Mejora el cumplimiento normativo con los mandatos de cuantificación del riesgo cibernético de GDPR, NIS2, DORA y SEC.
- Mejora la toma de decisiones a nivel directivo utilizando análisis de riesgos basados en datos.

Mapa de calor

Para visualizar el riesgo actual, inherente y residual en un mapa de calor, definimos cada tipo de riesgo:

- **Riesgo inherente:** El nivel de riesgo antes de aplicar cualquier control o medida de mitigación.
- **Riesgo actual:** El nivel de riesgo con los controles de seguridad existentes, pero antes del tratamiento adicional del riesgo.
- **Riesgo residual:** El riesgo restante tras aplicar mejoras de ciberseguridad.

RIESGO INHERENTE					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro					1
Probable					
Posible					
Improbable					
Raro					

Riesgos Extremos	1
Riesgos Altos	0
Riesgos Moderados	0
Riesgos Bajos	0
TOTAL RIESGOS	1

1 **ID del Escenario de Riesgo**

RIESGO ACTUAL					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro					
Probable				1	
Posible					
Improbable					
Raro					

Riesgos Extremos	0
Riesgos Altos	1
Riesgos Moderados	0
Riesgos Bajos	0
TOTAL RIESGOS	1

1 **ID del Escenario de Riesgo**

RIESGO RESIDUAL					
PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
Casi seguro					
Probable					
Posible					
Improbable			1		
Raro					

Riesgos Extremos	0
Riesgos Altos	0
Riesgos Moderados	1
Riesgos Bajos	0
TOTAL RIESGOS	1

1 **ID del Escenario de Riesgo**

Interpretación del mapa de calor

Nivel de Riesgo	Probabilidad	Impacto	Nivel
Riesgo inherente (Controles previos)	Casi seguro (80%)	Catastrófico ($100M+)	Extremo
Riesgo actual (con la seguridad existente)	Probable (60%)	Mayor ($50M-$80M)	Alto
Riesgo residual (Tras la detección basada en IA, copias de seguridad, ampliación del SOC)	Improbable (30%)	Moderado ($20M-$40M)	Moderado

Ahora vuelvo a valorar el cálculo del retorno de la inversión (ROI) de los controles de ciberseguridad aplicando un enfoque de modelización financiera.

El Banco invierte 2,5 millones de dólares en controles de ciberseguridad, incluyendo:

- Detección de amenazas basada en IA
- Cortafuegos avanzados
- Formación de los empleados
- Mejoras en la respuesta a incidents

Antes de implementar estos controles, la **expectativa de pérdida anual (ALE)** estimada por incidentes cibernéticos era de 6 millones de dólares.

Tras implantar los controles, la nueva ALE estimada es de 2 millones de dólares, lo que supone una reducción del riesgo de 4 millones de dólares.

Calculando el ROI

$$\boldsymbol{ROI = \frac{\text{Risk Reduction} - \text{Cost of Controls}}{\text{Cost of Control}} \times 100\%}$$

$$\boldsymbol{ROI = \frac{(6\ \text{M} - 2\text{M}) - 2,5\ \text{M}}{2,5\ \text{M}} \times 100\%}$$

$$\boldsymbol{ROI = \frac{(4\ \text{M} - 2,5\ \text{M})}{2,5\ \text{M}} \times 100\%}$$

$$\boldsymbol{ROI = \frac{1,5\ \text{M}}{2,5\ \text{M}} \times 100\%}$$

$$\boldsymbol{ROI = 60\ \%}$$

Aquí vemos que la inversión en ciberseguridad tiene un ROI del 60%, lo que significa que cada dólar gastado genera 1,60 dólares de valor al reducir las pérdidas relacionadas con la ciberseguridad.

Lo que a su vez el banco evita una pérdida anual de 4 millones de dólares gastando 2,5 millones, lo que justifica la inversión.

Simulación Monte Carlo para el ROI del ciberriesgo

Después de ejecutar 10.000 simulaciones, el ROI de ciberseguridad es:

- **ROI medio:** ~59,5% (Se alinea con nuestro cálculo manual).
- **Percentil 10 (Peor caso):** ~2,7% (Reducción del riesgo menor de lo esperado).
- **Percentil 90 (Mejor caso):** ~117,6% (Reducción significativa de las ciberpérdidas).

Valoración

- La inversión en ciberseguridad ofrece sistemáticamente un ROI positivo en la mayoría de los escenarios.
- En el peor de los casos, el ROI sigue siendo ligeramente positivo, lo que significa que la inversión no genera pérdidas financieras.
- En el mejor de los casos, el ROI más que duplica la inversión inicial.