UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas /UPV

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Facultad de Administración y Dirección de Empresas

Ciberseguridad y mercado bursátil: efecto de los ciberataques en empresas cotizadas

Trabajo Fin de Grado

Grado en Administración y Dirección de Empresas

AUTOR/A: Veliz García, Alonso

Tutor/a: Barrachina Martínez, Isabel

CURSO ACADÉMICO: 2025/2026

Agradecimientos

A mis padres, por ilusionarse tanto como yo con cada logro conseguido.

A mis amigos —Robert, Sandra, Mariano, Javi, Fabián, Denia, Cristian y Fidel— por acompañarme durante todos estos años.

A mi familia, porque cada avance es de todos nosotros.

A mi tutora Isabel, por ser de gran ayuda para la realización de este proyecto.

Y, sobre todo, a mi tío Rafa y mis abuelos, que seguro que me estáis animando desde allí arriba.

Este trabajo es tanto por mí como por vosotros. Os quiero.

Resumen

Este estudio cuantifica el impacto financiero de los ciberataques en empresas cotizadas, demostrando una destrucción de valor media del -6.84 % en los 10 días posteriores al anuncio del incidente. Mediante un estudio de eventos sobre 26 casos en los principales índices bursátiles, y la validación con un grupo de control, se aísla el efecto causal del ataque. Los resultados revelan un impacto negativo estadísticamente significativo, con la caída más pronunciada en el quinto día post-evento. Además, se constata un aumento del riesgo percibido, con un incremento significativo de la volatilidad en el 35 % de la muestra. El análisis diferencial muestra que el mercado penaliza con mayor severidad los ataques que interrumpen la operativa, mientras que las filtraciones de datos generan un mayor aumento de la incertidumbre (volatilidad). Estos hallazgos aportan evidencia empírica rigurosa de que los ciberataques se traducen en un riesgo financiero tangible, reforzando la necesidad de tratar la ciberseguridad como una inversión de capital (CAPEX) estratégica y no como un mero gasto operativo.

Palabras clave: Estudio de eventos, Retornos Anormales, Volatilidad, Nasdaq, Riesgo Financiero, Ciberataques

Resum

Aquest estudi quantifica l'impacte financer dels ciberatacs en empreses cotitzades i demostra una destrucció de valor mitjana del -6.84% en els 10 dies posteriors a l'anunci de l'incident. Mitjançant un estudi d'esdeveniments sobre 26 casos en els principals índexs borsaris i la validació amb un grup de control, s'aïlla l'efecte causal de l'atac. Els resultats revelen un impacte negatiu estadísticament significatiu, amb la caiguda més pronunciada el cinqué dia post-esdeveniment. A més, es constata un augment del risc percebut, amb un increment significatiu de la volatilitat en el 35% de la mostra. L'anàlisi diferencial mostra que el mercat penalitza amb més severitat els atacs que interrompen l'operativa, mentre que les filtracions de dades generen un augment més gran de la incertesa (volatilitat). Aquestes troballes aporten evidència empírica rigorosa que els ciberatacs es tradueixen en un risc financer tangible, reforçant la necessitat de tractar la ciberseguretat com una inversió de capital (CAPEX) estratègica i no com una simple despesa operativa.

Paraules clau: Estudi d'Esdeveniments, Retorns Anormals, Volatilitat, Nasdaq, Risc Financer, Ciberatacs

Abstract

This study quantifies the financial impact of cyberattacks on publicly traded companies, demonstrating an average value destruction of -6.84% in the 10 days following an incident's disclosure. Using an event study methodology on 26 incidents from major stock indices, validated against a control group, the causal effect of the attack is isolated. The findings reveal a statistically significant negative impact, with the sharpest decline on the fifth post-event day. Furthermore, a significant increase in perceived risk is observed, with volatility rising in 35% of the sample. Differential analysis shows that the market more severely penalizes attacks that disrupt operations, whereas data breaches lead to a greater increase in uncertainty (volatility). These findings provide rigorous empirical evidence that cyberattacks translate into tangible financial risk, reinforcing the need to treat

cybersecurity as a strategic capital expenditure (CAPEX) rather than a mere operating expense.

Key words: Event Study, Abnormal Returns, Volatility, Nasdaq, Financial Risk, Cyberattacks

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1
Introducción

1.1 Contexto general del tema

Resulta difícil encontrar hoy en día una empresa que no dependa, en mayor o menor medida, de algún tipo de infraestructura digital para llevar a cabo sus operaciones. Sistemas ERP, plataformas en la nube o el intercambio electrónico de datos han pasado de ser ventajas competitivas a requisitos básicos de funcionamiento [1, 2]. Gracias a estas herramientas, las organizaciones han logrado automatizar tareas, reducir costes operativos [3, 4] y, sobre todo, tomar decisiones más informadas al disponer de grandes volúmenes de datos históricos [5].

Sin embargo, esta misma dependencia ha generado un efecto colateral que no siempre recibe la atención que merece: cuanto más digitalizadas están las operaciones de una empresa, mayor es la superficie de ataque que ofrece a actores maliciosos [6]. La razón de fondo es sencilla: la información corporativa -desde datos de clientes hasta propiedad intelectual- constituye un activo de alto valor estratégico y, por tanto, un objetivo permanente para quienes buscan obtener un beneficio ilícito [7].

A este escenario se suma el auge de la inteligencia artificial. Si bien estas tecnologías están transformando sectores enteros, también presentan un riesgo considerable cuando son utilizadas con fines ofensivos [8, 9]. Los atacantes disponen ahora de herramientas para diseñar ataques más sofisticados y difíciles de detectar. Y aunque muchas organizaciones han reforzado sus defensas, la realidad es que los ataques han evolucionado a un ritmo que, en muchos casos, supera la capacidad de respuesta de las propias empresas [10, 11]. Todo ello se desarrolla en un contexto geopolítico marcado por la inestabilidad, que contribuye a amplificar el riesgo sistémico a escala global [12]. De hecho, según el informe *Global Cybersecurity Outlook 2025* del World Economic Forum [13], el 72 % de las organizaciones consultadas afirmaron haber percibido un incremento de los riesgos cibernéticos durante el último año.

Las consecuencias económicas de esta amenaza también se están acelerando. El informe *Cost of a Data Breach 2024* de IBM sitúa el coste medio de una brecha de datos en 4,88 millones de dólares, un 10 % más que el año anterior y la cifra más alta registrada hasta la fecha [14]. Una parte significativa de este incremento se explica por las pérdidas de negocio: los clientes pierden la confianza en la organización afectada, lo que erosiona la base de ingresos y deteriora la imagen corporativa. A estos costes se añaden los derivados de la respuesta al incidente: investigaciones forenses, comunicación de crisis y la implantación de nuevas medidas de seguridad.

Todo lo anterior apunta a una conclusión clara: la ciberseguridad ya no puede tratarse como un asunto confinado al departamento técnico, sino que se ha convertido en una prioridad estratégica de primer orden [15]. Entender su impacto desde la óptica financiera resulta esencial para empresas, inversores, analistas y gestores de riesgo. Precisamente por ello, examinar cómo reaccionan los mercados financieros cuando se hace público un ciberataque permite poner cifras a un riesgo que, hasta hace poco, se gestionaba de forma más intuitiva que cuantitativa.

1.2 Planteamiento del problema

Los mercados financieros son altamente sensibles a la nueva y relevante información [16]. Eventos como resultados electorales, cambios en la política monetaria o decisiones estratégicas de grandes empresas pueden provocar reacciones inmediatas por parte de los inversores [17], traduciéndose en variaciones significativas en los precios de los activos.

En este contexto, la difusión de una noticia relacionada con un incidente de ciberseguridad en una empresa cotizada puede ser interpretada como una señal de vulnerabilidad estructural o de deficiencias en la gestión de riesgos [18, 19]. Como se puede ver en la figura 1.1, esta percepción negativa puede desencadenar respuestas rápidas en el mercado, reflejadas en caídas del precio de la acción, aumentos en la volatilidad o alteraciones en el volumen de negociación. No obstante, existe la duda de que la magnitud y duración de estas reacciones no sean uniformes y puedan variar según el tipo de ataque, el sector afectado, la capacidad de respuesta de la empresa o el contexto económico general. Esto sugiere la existencia de factores que deben ser estudiados.

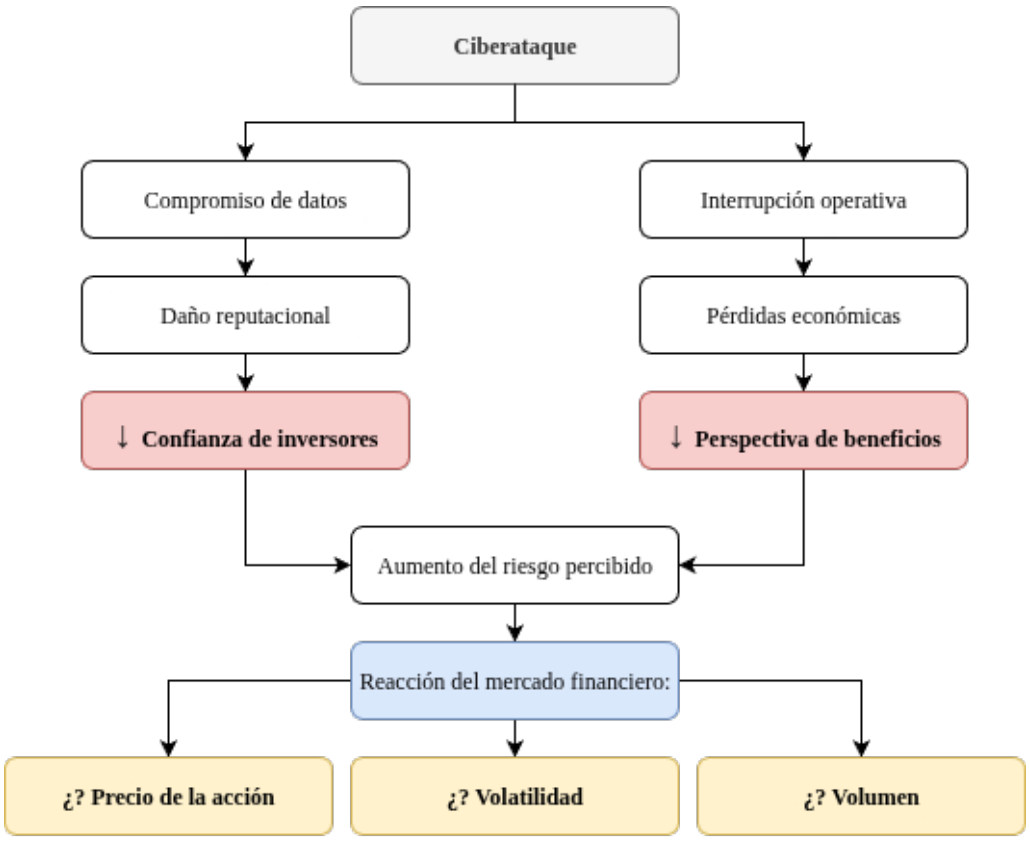

Figura 1.1: *Cadena previsible del impacto financiero derivado de un ciberataque. Fuente: elaboración propia*

Por tanto, surge la necesidad de abordar el problema de manera empírica, con el objetivo de cuantificar cómo y en qué medida los ciberataques afectan al valor de las empresas cotizadas. El principal desafío consiste en aislar el efecto atribuible exclusivamente al incidente de seguridad. Además, es fundamental examinar si estos eventos implican un cambio estructural en la percepción del riesgo por parte de los inversores, lo cual se manifestaría en alteraciones en la volatilidad y en otros indicadores de incertidumbre financiera.

1.3 Justificación del trabajo

El presente trabajo se justifica por tres razones principales: la actualidad y relevancia del fenómeno, la creciente presión institucional para crear una infraestructura capaz de responder a los incidentes de ciberseguridad, y la utilidad práctica de los resultados obtenidos por parte de directivos, inversores y analistas.

En primer lugar, los ciberataques han dejado de ser hechos aislados para convertirse en una amenaza recurrente con implicaciones operativas, reputacionales y financieras [19, 20]. Solo en 2024 se registraron más de `100.000` ciberincidentes en España, de los cuales, cada tres días, al menos uno fue considerado grave o crítico según datos del Ministerio para la Transformación Digital y de la Función Pública [21]. Esta realidad ha motivado una respuesta política contundente, incluyendo la necesidad de redefinir el Plan de Ciberseguridad Nacional aprobado el 29 de mayo de 2022. Realizando así un nuevo plan de inversión pública superior a los `1.100` millones de euros destinado a reforzar la resiliencia digital del país.

En segundo lugar, aunque, según palabras del ministro de Transformación Digital y de la Función Pública, Óscar López, España ya se posiciona como "un ejemplo a seguir en materia de ciberseguridad" -siendo el segundo país del mundo con mayor número de centros especializados-, el compromiso institucional va más allá. El Gobierno ha manifestado su voluntad de seguir avanzando en la protección de los derechos digitales de la ciudadanía, en la garantía de la estabilidad económica y en la defensa de la soberanía del Estado en el entorno digital [21]. Esta ambición refuerza la necesidad de contar con un marco de análisis sólido que permita comprender el impacto económico de los ciberataques y orientar la toma de decisiones estratégicas tanto en el ámbito público como en el privado.

Por último, los resultados de esta investigación pueden ser de utilidad práctica para distintos perfiles profesionales: analistas financieros, inversores, responsables de cumplimiento normativo y gestores de riesgos. Conocer la magnitud y duración de las reacciones del mercado ante incidentes de ciberseguridad permite valorar mejor la exposición al riesgo y diseñar estrategias preventivas basadas en evidencia empírica. Asimismo, esta información resulta valiosa para los equipos directivos, al ofrecer argumentos sólidos que justifiquen la inversión en ciberseguridad como parte del *CAPEX* (gasto de capital) de la organización, desde una perspectiva tanto financiera como estratégica.

En definitiva, este trabajo pretende aportar conocimiento útil, oportuno y accionable en un contexto en el que la intersección entre tecnología, finanzas y estrategia empresarial es cada vez más relevante.

1.4 Objetivos

El objetivo general de este Trabajo de Fin de Grado es **cuantificar el impacto financiero de los incidentes de ciberseguridad en las empresas cotizadas**, evaluando cómo reaccionan los mercados de valores ante las noticias de este tipo de eventos.

De este objetivo principal se derivan los siguientes objetivos específicos:

- Estimar los **retornos anormales** (AR) y los **retornos anormales acumulados** (CAR) mediante la metodología de estudios de eventos, utilizando el modelo CAPM para determinar el impacto inmediato y prolongado de los ciberataques en el valor de mercado de las empresas afectadas.
- Analizar los cambios en la **percepción de riesgo** del mercado mediante el estudio de la volatilidad en dos dimensiones: la **volatilidad realizada** para medir cambios en el nivel de riesgo, y la **volatilidad condicional** mediante modelos GARCH(1,1) para evaluar la persistencia temporal de los shocks.
- Validar la **causalidad del impacto** comparando la evolución de las empresas afectadas con un grupo de control de competidores directos no afectados, aislando así el efecto específico atribuible al ciberataque.
- Identificar **factores determinantes** de la magnitud del impacto, analizando si la reacción del mercado varía según: la naturaleza del ataque (filtraciones de datos vs. ataques operacionales), el sector económico (tecnología, finanzas, salud, etc.), y el mercado de cotización (NASDAQ vs. NYSE).
- Cuantificar la **destrucción de valor** para el accionista y su horizonte temporal, determinando si el impacto es transitorio o persistente mediante el análisis de múltiples ventanas temporales (corto, medio y largo plazo).
- Derivar **implicaciones prácticas** para la toma de decisiones, traduciendo los hallazgos empíricos en recomendaciones concretas para: la justificación económica del CAPEX en ciberseguridad, la gestión de crisis post-incidente, y la incorporación del riesgo cibernético en modelos de valoración de activos.

1.5 Estructura del documento

El documento se estructura en 9 capítulos principales, seguidos de una bibliografía y los correspondientes anexos. A continuación, se presenta el contenido de cada uno de los capítulos:

- **Capítulo 1: Introducción**. En este capítulo se ha presentado el objeto de estudio del proyecto: analizar el impacto financiero de los incidentes de ciberseguridad en empresas cotizadas. Asimismo, se han definido los objetivos generales y específicos de la investigación. También se contextualiza la relevancia del tema, destacando el papel creciente de la ciberseguridad como un factor estratégico clave con implicaciones financieras directas.
- **Capítulo 2: Marco teórico**. Se presentan los fundamentos teóricos necesarios para comprender la metodología empleada. El capítulo aborda conceptos clave como la hipótesis de eficiencia de mercados, la metodología de estudios de eventos, los modelos de valoración de activos y el análisis de volatilidad. Además, se revisa la

literatura existente sobre el impacto bursátil de los ciberataques, estableciendo el estado del arte en este campo de investigación.

- **Capítulo 3: Marco práctico**. Este capítulo analiza el contexto actual de la ciberseguridad empresarial desde una perspectiva aplicada. Se identifican las tipologías de ataques más frecuentes, sus costes asociados y tiempos de detección. También se examina el impacto económico, legal y reputacional de estos incidentes, así como su relación con la evolución reciente de los mercados financieros, proporcionando el contexto necesario para interpretar los resultados del análisis empírico.

- **Capítulo 4: Metodología**. En el cuarto capítulo se detalla el proceso metodológico seguido en la investigación. El capítulo describe la selección de la muestra de ciberataques analizados, los criterios de inclusión y exclusión aplicados, las herramientas computacionales utilizadas (Python y sus librerías especializadas), y la implementación práctica de los modelos econométricos. Se explican paso a paso los procedimientos para el cálculo de retornos anormales y el análisis de volatilidad.

- **Capítulo 5: Presentación de los resultados**. En este capítulo se exponen los hallazgos obtenidos tras aplicar la metodología descrita. Se presentan los retornos anormales acumulados (CAR) para diferentes ventanas temporales, los cambios en la volatilidad realizada y condicional, y se analizan los resultados segmentados por sector económico, tipo de ataque y mercado de cotización. Además, se incluye un caso ilustrativo detallado para facilitar la comprensión del proceso analítico.

- **Capítulo 6: Discusión de los resultados**. Se interpretan los hallazgos en relación con los objetivos planteados y se contrastan con la literatura previa. El capítulo analiza el impacto causal de los ciberataques en el valor de mercado, identifica los factores que modulan la reacción bursátil, y extrae las implicaciones prácticas tanto para la gestión empresarial como para las decisiones de inversión.

- **Capítulo 7: Propuestas de mejora**. A partir del análisis realizado, se plantean mejoras metodológicas y líneas de investigación futuras que podrían complementar y ampliar los hallazgos de este trabajo.

- **Capítulo 8: Conclusiones**. Para terminar con el análisis, se sintetizan los principales hallazgos de la investigación, se discuten las limitaciones del estudio y se proponen direcciones para investigaciones posteriores que puedan profundizar en esta temática.

- **Capítulo 9: Relación del trabajo con los objetivos de desarrollo sostenible (ODS)**. Se analiza la vinculación del presente trabajo con los Objetivos de Desarrollo Sostenible de la Agenda 2030, identificando y justificando el grado de relación con cada uno de ellos.

- **Bibliografía y Anexos**. Se incluyen las fuentes bibliográficas consultadas y material adicional de soporte como tablas, gráficos o el código empleado.

CAPÍTULO 2
Marco teórico

Este capítulo presenta los fundamentos conceptuales y metodológicos que sustentan el análisis desarrollado en este trabajo. La revisión teórica se organiza en cinco bloques temáticos: la eficiencia de los mercados, los estudios de eventos, los modelos de valoración de activos, el análisis de la volatilidad y, por último, la evidencia empírica existente sobre la reacción bursátil ante ciberataques.

El propósito de esta estructura es proporcionar un marco analítico sólido que permita comprender cómo y por qué los mercados financieros reaccionan ante la divulgación de eventos inesperados. De este modo, se sientan las bases necesarias para la aplicación empírica posterior.

El orden elegido responde a un criterio lógico y progresivo: desde los principios generales de eficiencia y valoración hasta los enfoques específicos para medir y analizar la reacción del mercado ante eventos disruptivos. La revisión culmina con el trabajo de Celeny et al. [22], que representa una de las contribuciones más recientes y relevantes en el campo.

2.1 Hipótesis de eficiencia y reacción del mercado

Para comprender cómo y por qué los mercados financieros reaccionan ante eventos inesperados como los ciberataques, es fundamental comenzar hablando de la teoría de la eficiencia de mercados, desarrollada por el premio Nobel Eugene Fama [16]. Esta teoría constituye el pilar conceptual que justificará el uso de los estudios de eventos como metodología de análisis.

Fama plantea que en un **mercado eficiente**, los precios de **los activos reflejan de forma completa y rápida toda la información disponible**. La competencia entre inversores conduce a un equilibrio donde el precio de mercado representa una estimación del valor intrínseco de los activos. Esta premisa implica que **cualquier nueva información relevante se incorporará inmediatamente en los precios**, sin posibilidad de obtener rentabilidades anormales de forma sistemática.

Su teoría distingue tres niveles de eficiencia según el conjunto de información que se refleje en los precios. Este trabajo se fundamenta específicamente en la **hipótesis de eficiencia en forma semifuerte**, que constituye el supuesto teórico más relevante para los estudios de eventos. Bajo esta forma de eficiencia, **los precios reflejan toda la información públicamente disponible**, incluyendo estados financieros, comunicados de prensa, noticias económicas y otros datos de dominio público. Es por ello que un mercado debería reaccionar de manera inmediata ante la divulgación pública de un ciberataque, incorporando instantáneamente las implicaciones del mismo en el precio de la acción

afectada. En consecuencia, **la posible variación en los precios tras la divulgación de un ciberataque podría interpretarse como una medida del impacto del mismo**.

Si bien la hipótesis de eficiencia ha sido objeto de críticas y revisiones posteriores, incluso por el propio Fama en un artículo posterior [23]. O también por la presencia de anomalías, como el denominado *efecto enero*, según el cual las rentabilidades obtenidas durante el mes de enero tienden, de forma consistente, a superar las ganancias registradas en el resto del año [24]. La hipótesis de eficiencia semifuerte sigue siendo el marco teórico predominante para interpretar el comportamiento de los mercados financieros frente a eventos inesperados, debido a su capacidad para ofrecer una base coherente y contrastable empíricamente.

2.2 Los estudios basados en eventos

Ahora que hemos definido que el trabajo se sostiene en la hipótesis de eficiencia en su forma semifuerte, podemos asumir que los mercados reaccionarán ante la aparición de nueva información relevante. ¿Pero en qué cuantía? ¿La reacción es realmente significativa o una mera perturbación despreciable?

En este contexto, la **metodología de estudios basados en eventos** (*event studies*) se presenta como una herramienta ampliamente utilizada en finanzas para medir la reacción del mercado ante sucesos concretos. Ball y Brown [25] fueron pioneros en dicha metodología, que fue formalizada posteriormente por Fama [26]. Desde entonces, se ha consolidado como un enfoque estándar para evaluar el impacto de eventos como anuncios de resultados, fusiones, cambios regulatorios, decisiones judiciales o, como en nuestro caso, incidentes de ciberseguridad, sobre los valores financieros [27].

Para su definición, nos apoyaremos principalmente en el capítulo 12.5 del libro *Financial Trading and Investing* de John L. Teall [28], junto con el resto de fuentes complementarias listadas en la bibliografía. El **objetivo** central de esta metodología es **determinar si existe una reacción estadísticamente significativa** en los precios (u otras variables financieras, como la volatilidad o el volumen de negociación) **en torno al momento en que se da a conocer el evento**.

Como valor añadido, además de su valor teórico, desde una perspectiva práctica o de *trading*, los estudios de eventos permiten realizar **pruebas retrospectivas** (back-testing) para evaluar la rentabilidad y fiabilidad de estrategias de inversión basadas en la anticipación o reacción a este tipo de sucesos [28].

2.2.1. Fundamentos del análisis de eventos

Es fundamental comprender que la metodología de estudios de eventos no es monolítica. Dependiendo de la variable financiera que se busque analizar —como podrían ser los retornos o la volatilidad en nuestro caso— el diseño del estudio y la estructura temporal empleada difieren sustancialmente. Esta distinción metodológica responde a la naturaleza intrínseca de cada variable y a los modelos disponibles para su análisis.

En primer lugar, vamos a hablar del análisis de la **rentabilidad**. En el que el objetivo va a ser detectar desviaciones respecto a un comportamiento esperado, lo que requerirá de un modelo de referencia y de ventanas temporales específicas para su estimación. Por otro lado, el análisis de **volatilidad** busca identificar cambios en el nivel o estructura del riesgo, empleando comparaciones directas o modelos dinámicos que no requieren la misma estructura temporal.

Esta diferencia fundamental debe tenerse presente a lo largo de todo el estudio, ya que va a determinar tanto los procedimientos de cálculo como la interpretación de los resultados.

2.2.2. Análisis de rentabilidades: estructura temporal y ventanas de cálculo

Cuando el objetivo es medir el impacto del ciberataque sobre la **rentabilidad** de las acciones, el análisis se estructura en torno a tres ventanas temporales específicas, las cuales se pueden observar en la figura 2.1, y que son:

- **Ventana de estimación**: Período anterior al evento (típicamente 120-252 días bursátiles) utilizado para calibrar los modelos de mercado. Modelos de mercado, que son utilizados para calcular las rentabilidades esperadas en ausencia del evento. En esta ventana se debe evitar el solapamiento con la ventana del evento para prevenir contaminación estadística con los días en los que se espera que el suceso provoque efectos en las variables analizadas. [17, 29].

- **Ventana del evento**: Período en que se espera la reacción del mercado, centrado en la fecha de anuncio. Su amplitud depende de la naturaleza del evento y del periodo que busquemos analizar el impacto (por ejemplo, $t = -1$ a $t = +1$). Una práctica muy común en estudios de eventos es estudiar diferentes ventanas temporales, para comprobar en qué rango los acontecimientos producen efectos significativos en las variables estudiadas y cuánto se extienden las perturbaciones.

- **Ventana de análisis posterior**: opcional. Permite evaluar la persistencia o reversión del impacto inicial (por ejemplo, en una ventana de evento de $t = -1$ a $t = +1$ podemos analizar desde $t = +2$ a $t = +10$ días después de la ventana del evento).

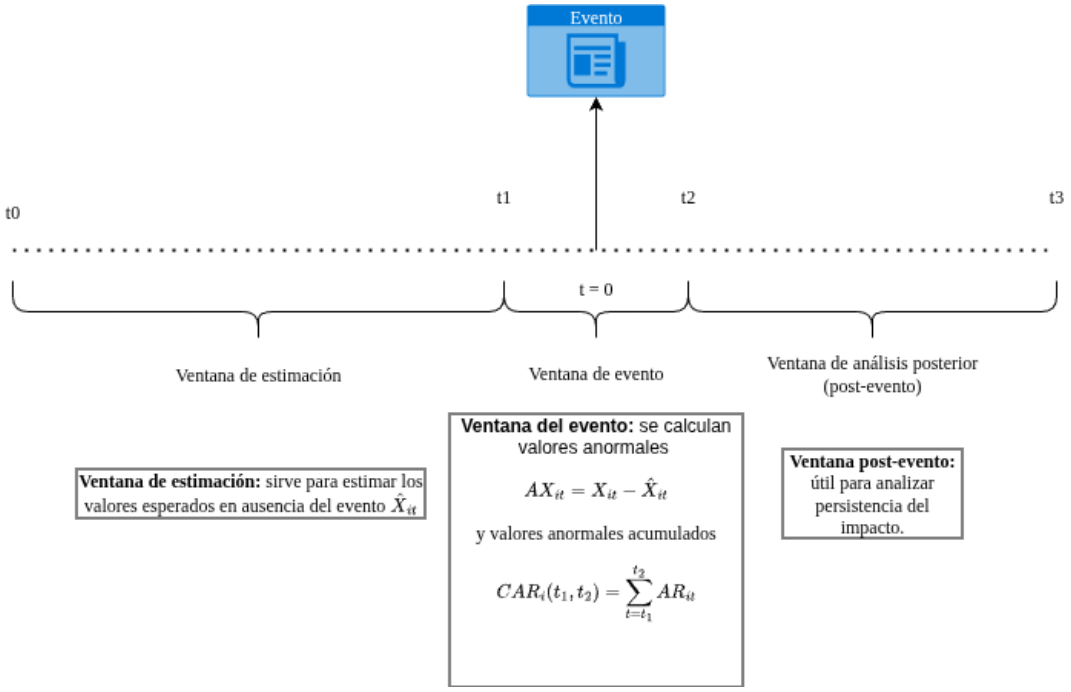

Figura 2.1: *Ventanas del análisis de eventos. Fuente: elaboración propia*

2.2.3. Cálculo de rentabilidades anormales

El concepto central en el análisis de rentabilidades es la **rentabilidad anormal** (AR), que representa la diferencia entre el retorno observado de un activo y el retorno que se habría esperado en ausencia del evento.

Formalmente, la rentabilidad anormal se define como:

$$AR_{it} = R_{it} - \hat{R}_{it} \tag{2.1}$$

donde:

- AR_{it}: rentabilidad anormal del activo i en el día t
- R_{it}: rentabilidad observada del activo
- $\hat{R}_{it}$: rentabilidad esperada, estimado mediante un modelo de valoración de activos

El retorno esperado $\hat{R}_{it}$ se obtiene aplicando los parámetros estimados durante la ventana de estimación a las condiciones de mercado observadas durante la ventana del evento. Por ejemplo, utilizando el modelo CAPM:

$$\hat{R}_{it} = \hat{\alpha}_i + \hat{\beta}_i R_{mt} \tag{2.2}$$

donde:

- $\hat{\alpha}_i$ y $\hat{\beta}_i$ son los parámetros estimados mediante regresión durante la ventana de estimación,
- R_{mt} es el retorno del mercado en el día t de la ventana del evento.

2.2.4. Cálculo de rentabilidades anormales acumuladas

Para capturar el impacto acumulado del evento a lo largo de varios días, se calcula la **rentabilidad anormal acumulada** (Cumulative Abnormal Return, CAR):

$$CAR_i(t_1, t_2) = \sum_{t=t_1}^{t_2} AR_{it} \tag{2.3}$$

El CAR es particularmente útil porque los efectos de un evento pueden no manifestarse completamente en un solo día. Un ciberataque anunciado un viernes por la tarde, por ejemplo, podría ver su impacto el lunes siguiente cuando el mercado reabre. Además, la información puede ser procesada gradualmente por los inversores, especialmente si las implicaciones del ataque no son inmediatamente claras.

2.3 Modelos para la estimación de retornos esperados

Para calcular los retornos anormales, es necesario primero modelar la rentabilidad esperada en ausencia del evento. Los modelos más utilizados en la literatura son el CAPM y el modelo de tres factores de Fama-French.

2.3.1. Modelo de mercado (CAPM).

El Capital Asset Pricing Model (CAPM) es el modelo más empleado en estudios de eventos por su simplicidad y robustez [30, 17]. Establece que la rentabilidad esperada de un activo depende de su sensibilidad al riesgo sistemático del mercado. Se define como sigue:

$$E(R_{it}) = R_{ft} + \beta_i(E(R_{mt}) - R_{ft}) \tag{2.4}$$

donde:

- $E(R_{it})$: retorno esperado del activo i en el periodo t,
- R_{ft}: tasa libre de riesgo en el periodo t,
- β_i: coeficiente de sensibilidad del activo al mercado (riesgo sistemático),
- $E(R_{mt})$: retorno esperado del mercado en el periodo t.

En la práctica empírica, y más concretamente en el caso que nos ocupa, los estudios de eventos a corto plazo, se suele utilizar una versión lineal estimada a través de regresión:

$$R_{it} = \alpha_i + \beta_i R_{mt} \tag{2.5}$$

donde:

- R_{it}: retorno observado del activo i en el periodo t,
- R_{mt}: retorno observado del mercado en el mismo periodo t,
- α_i: término constante, que representa el rendimiento no explicado por el mercado,
- β_i: representa la sensibilidad del activo al mercado (riesgo sistemático).

Esta simplificación es válida porque la tasa libre de riesgo diaria es prácticamente despreciable en ventanas cortas. Los parámetros α_i y β_i se estiman mediante mínimos cuadrados ordinarios (MCO) durante la ventana de estimación.

Este procedimiento consiste en encontrar los valores de α_i y β_i que minimizan la suma de los cuadrados de los residuos, es decir, la diferencia entre los rendimientos observados del activo y los rendimientos que predice el modelo:

$$\min_{\alpha,\beta} \sum_{t=1}^{T} (R_{it} - \alpha - \beta R_{mt})^2 \tag{2.6}$$

Donde:

- R_{it}: retorno observado del activo i en el día t,
- R_{mt}: retorno del mercado en el día t,
- T: número de observaciones dentro de la ventana de estimación.

2.3.2. Modelo de tres factores de Fama-French

Aunque este trabajo emplea el CAPM por simplicidad, cabe mencionar brevemente el modelo de tres factores de Fama-French [31, 32] como alternativa más sofisticada. Este modelo añade al CAPM dos factores adicionales: SMB (Small Minus Big), que captura la prima por tamaño, y HML (High Minus Low), que refleja la prima por valor.

Estudios recientes, como el ya mencionado de Celeny et al. [22] emplean este modelo por su mayor capacidad explicativa. Sin embargo, para los objetivos de este proyecto, el CAPM proporciona una aproximación suficiente, evitando la complejidad adicional que supone obtener y procesar los factores SMB y HML.

2.4 Volatilidad y percepción del riesgo

Además del análisis del retorno, resulta pertinente evaluar el impacto del evento sobre la **volatilidad**, entendida como una medida de la incertidumbre o del riesgo percibido por los inversores.

Dado que el binomio rentabilidad-riesgo sugiere que un aumento en la rentabilidad implicará una mayor volatilidad (y viceversa), va a ser necesario cuantificar empíricamente dichas variaciones. En el caso de un ciberataque, es razonable suponer que los inversores revisarán al alza el perfil de riesgo de la empresa afectada, lo que puede reflejarse en una mayor dispersión de los precios de sus activos.

Es crucial entender que, a diferencia del análisis de rendimientos, no calculamos una "volatilidad anormal" respecto a un modelo de equilibrio. En su lugar, evaluamos **cambios en el nivel o estructura de la volatilidad** mediante comparaciones directas o modelos dinámicos.

En el análisis, se van a utilizar dos enfoques complementarios: la **volatilidad realizada o histórica** y la **volatilidad condicional**.

2.4.1. Volatilidad realizada

La **volatilidad realizada** es una medida empírica de la variabilidad de los retornos **históricos**. Se calcula como la desviación estándar de una serie temporal de rentabilidades diarias, y suele expresarse en términos anualizados.

$$\sigma_t^{\text{realizada}} = \text{std}(r_{t-n+1}, \ldots, r_t) \cdot \sqrt{252} \tag{2.7}$$

Donde:

- $\sigma_t^{\text{realizada}}$: Volatilidad realizada estimada en el día t, expresada en términos anualizados.
- $\text{std}(r_{t-n+1}, \ldots, r_t)$: Desviación estándar muestral de los retornos diarios en una ventana de n días. [33]
- r_t: Retorno diario del activo en el día t.
- $\sqrt{252}$: Factor de anualización, asumiendo 252 días bursátiles al año. Esta conversión permite comparar niveles de volatilidad entre diferentes horizontes temporales.

Para evaluar el impacto del ciberataque, comparamos la volatilidad antes y después del evento:

$$\Delta\sigma = \sigma_{\text{post}} - \sigma_{\text{pre}}$$

Un $\Delta\sigma$ positivo indicará que el mercado percibe mayor riesgo tras el evento.

2.4.2. Volatilidad condicional: modelo GARCH(1,1)

El análisis de la volatilidad realizada ofrece una visión estática, limitada a una ventana temporal específica, sería comparable con una "foto fija", que compara el antes y el después. Sin embargo, desde la perspectiva de los inversores, resulta crucial comprender si el aumento del riesgo tras un evento adverso —como un ciberataque— es transitorio o persistente.

Esta distinción resulta fundamental en el contexto de este trabajo, ya que determinará si los ciberataques provocan un incremento puntual de la incertidumbre o si alteran de forma duradera el perfil de riesgo percibido por los inversores, con implicaciones directas para la valoración de activos y la gestión de carteras.

Para capturar este comportamiento dinámico, recurrimos a la **volatilidad condicional**, que representa la variabilidad esperada de los retornos en función de la información disponible hasta el momento.

Una característica empírica observada en los mercados financieros es la **heterocedasticidad condicional**: la volatilidad no es constante, sino que se agrupa en *rachas*. Es decir, los períodos de alta (o baja) volatilidad tienden a concentrarse en el tiempo. Los modelos GARCH fueron desarrollados por Engle [34] precisamente para modelar esta dependencia temporal de la varianza.

Estructura del modelo GARCH(1,1)

La especificación básica del modelo GARCH(1,1) consta de dos ecuaciones:

Ecuación de la media

$$r_t = \mu + \varepsilon_t \tag{2.8}$$

donde:

- r_t: retorno del activo en el día t,
- μ: media condicional del retorno (puede ser constante),
- ε_t: innovación o shock, con varianza no constante.

Ecuación de la varianza condicional El comportamiento dinámico de la volatilidad se describe mediante:

$$\sigma_t^2 = \omega + \alpha\varepsilon_{t-1}^2 + \beta\sigma_{t-1}^2 \tag{2.9}$$

donde:

- σ_t^2: varianza condicional del retorno en el día t,
- ω: constante que representa la varianza de largo plazo,

- α: efecto ARCH (impacto de shocks recientes),
- β: efecto GARCH (persistencia de la volatilidad pasada).

Esta formulación implica que la varianza actual depende tanto de la magnitud del shock anterior (ε_{t-1}^2) como del nivel de volatilidad observado el día anterior (σ_{t-1}^2).

Estimación del modelo

Una vez definida la estructura del modelo, el objetivo es encontrar los valores de los parámetros $\theta = (\mu, \omega, \alpha, \beta)$ que mejor se ajusten a los datos observados. A diferencia del modelo CAPM, donde los parámetros se estiman mediante mínimos cuadrados ordinarios, el modelo GARCH requiere un enfoque diferente. Esto se debe a que la varianza no es constante, sino que depende recursivamente de sus propios valores pasados: para calcular σ_t^2 necesitamos σ_{t-1}^2, que a su vez depende de σ_{t-2}^2, y así sucesivamente. Esta dependencia recursiva hace que el método de mínimos cuadrados no sea aplicable.

En su lugar, se recurre a la **estimación por máxima verosimilitud** (*Maximum Likelihood Estimation*, MLE). La idea es la siguiente: dado un conjunto de retornos observados, se buscan los valores de ω, α y β que maximicen la probabilidad de haber generado exactamente esos datos. Formalmente, esto equivale a maximizar la función de log-verosimilitud:

$$\mathcal{L}(\theta) = -\frac{1}{2}\sum_{t=1}^{T}\left[\log(2\pi) + \log(\sigma_t^2) + \frac{\varepsilon_t^2}{\sigma_t^2}\right]$$

La estimación se realiza de forma numérica mediante algoritmos de optimización, implementados en este trabajo a través de la librería `arch` de Python, por lo que no se requiere un desarrollo analítico adicional en esta sección.

Interpretación de parámetros

Los parámetros clave del modelo de GARCH son la suma $\alpha + \beta$, que refleja la **persistencia total** del proceso:

- Si $\alpha + \beta < 1$: el proceso es *estacionario*; los efectos de los shocks se disipan gradualmente.
- Si $\alpha + \beta \approx 1$: la persistencia es alta; la volatilidad tarda en volver a niveles normales.
- Si $\alpha + \beta = 1$: el proceso es *no estacionario*; los shocks tienen efectos permanentes.

Adicionalmente:

- Un valor elevado de α indica mayor sensibilidad a los shocks recientes.
- Un valor elevado de β sugiere mayor inercia en la volatilidad.

Así, dos activos con igual persistencia total pueden comportarse de forma distinta: uno puede reaccionar bruscamente pero estabilizarse rápido (alto α, bajo β), y otro mostrar una respuesta más lenta pero sostenida (bajo α, alto β).

En resumen, el modelo GARCH(1,1) permite capturar la naturaleza dinámica de la volatilidad y resulta especialmente útil para analizar si un evento genera un aumento transitorio o persistente en la percepción de riesgo [35].

2.5 Estudios previos: reacción del mercado ante ciberataques

Existe una extensa literatura en finanzas que documenta cómo los ciberataques constituyen *shocks exógenos* sobre el valor de mercado de las empresas afectadas [19], al alterar tanto las expectativas de los inversores como la percepción de riesgo asociada a la compañía.

Los primeros trabajos en esta línea se remontan a principios de la década de 2000. Cavusoglu et al. [18] analizaron 66 incidentes de seguridad entre 1998 y 2002, documentando un CAR medio del –0,86 % en ventanas de dos días y evidenciando que el mercado ya entonces diferenciaba entre tipos de ataque, penalizando con mayor severidad las intrusiones con acceso a datos frente a los ataques de denegación de servicio. Precisamente sobre estos últimos, Hovav y D'arcy [36] no encontraron un impacto bursátil significativo, al interpretarlos el mercado como interrupciones temporales sin consecuencias estructurales —un resultado que, como se discutirá más adelante, contrasta con los hallazgos de este trabajo para ataques operativos más recientes—.

Posteriormente, Goel y Shawky [37] ampliaron el análisis a 168 incidentes y documentaron, además del impacto directo sobre la empresa afectada, un efecto de contagio sectorial, observando retornos anormales negativos en competidores del mismo sector. Más recientemente, Kamiya et al. [20], en uno de los estudios más exhaustivos publicados hasta la fecha en el *Journal of Financial Economics*, analizaron más de 800 ciberataques y demostraron que las consecuencias trascienden el corto plazo bursátil, incluyendo cambios en la dirección ejecutiva y pérdida de cuota de mercado, siendo especialmente severas en empresas con deficiencias en su gobernanza corporativa.

Uno de los trabajos más recientes en esta línea es el de Celeny et al. [22], al que ya hemos hecho referencia en distintas secciones de este estudio. Los autores abren su investigación subrayando la creciente importancia de la ciberseguridad en el sistema financiero, a partir del ciberataque que afectó en noviembre de 2023 a la filial estadounidense del banco ICBC. Este incidente, que obligó al mayor banco del mundo a interrumpir temporalmente el procesamiento electrónico de transacciones del Tesoro de EE. UU., fue calificado como un "verdadero shock" por Marcus Murray, fundador de la firma de ciberseguridad Truesec.

El estudio de Celeny et al. aplica un event study a una muestra de 167 ciberataques sufridos por 73 empresas estadounidenses entre 2012 y 2022. La construcción de esta muestra siguió un procedimiento en dos fases.

En primer lugar, se recopiló información financiera de mercado a través de la API de Wharton Research Data Services (WRDS), filtrando únicamente aquellas empresas que hubieran registrado al menos un ciberincidente documentado. En segundo lugar, se recolectaron titulares de prensa mediante la plataforma Refinitiv Eikon, aplicando diversos filtros: idioma (inglés), localización (empresas norteamericanas), inclusión de palabras clave asociadas a ciberataques y validación semántica mediante modelos de Procesamiento del Lenguaje Natural (PLN), especialmente útil para titulares complejos. Este proceso permitió depurar un conjunto inicial de más de 100.000 titulares hasta identificar 270 eventos confirmados.

Para calcular los retornos anormales, los autores emplean el modelo de tres factores de Fama y French (FF3) y estiman los efectos sobre una ventana de evento de tres días en torno al incidente. Los retornos anormales se escalan y corrigen por sesgos comunes en estudios de eventos —como la varianza inducida por el evento y la correlación cruzada residual— aplicando los ajustes propuestos por [38].

Sus resultados revelan que no todos los ciberincidentes son castigados por igual por el mercado: mientras que la mayoría no genera una reacción estadísticamente significativa, aquellos clasificados como *data breaches* provocan una caída media de hasta el –1.3 % en el precio de las acciones durante los días posteriores al evento. El impacto es especialmente severo en el sector salud, donde las pérdidas pueden alcanzar el –5.2 %.

CAPÍTULO 3
Marco práctico

Una de las ideas más repetidas en el análisis contemporáneo de la sociedad —y que constituye también el punto de partida de este trabajo— es la siguiente: *la sociedad contemporánea está profundamente marcada por el proceso de digitalización acelerada iniciado a comienzos del siglo XXI* [39].

Basta con observar nuestro entorno para darnos cuenta de ello: estamos rodeados de dispositivos tecnológicos que procesan y transmiten nuestra información de forma continua. Esta integración en nuestra vida cotidiana es tan profunda que muchas veces la damos por sentada, olvidando que, probablemente, nuestros datos terminarán —o lo más seguro, ya han terminado— en manos de terceros, como grandes empresas, gobiernos o plataformas digitales, que hacen uso de ellos con fines comerciales, políticos o de control social [40].

Este ecosistema digital, si bien ha generado grandes avances, también ha incrementado significativamente nuestra exposición a riesgos cibernéticos [6]. Y si nos afecta a nosotros a nivel individual, el efecto es aún mayor a nivel empresarial.

3.1 Tipología de ciberataques más frecuentes en el entorno empresarial

No todos los ciberataques generan el mismo impacto financiero ni operativo. Aunque este trabajo analiza una tipología diversa de incidentes (incluyendo ataques de ransomware, denegaciones de servicio, vulnerabilidades críticas o ingeniería social), resulta útil tomar como referencia el informe de IBM [14], del que ya hemos hecho alusión en la introducción, y que está centrado específicamente en brechas de datos (*data breaches*), lo cual se debe a dos razones fundamentales.

En primer lugar, las brechas de datos constituyen una de las tipologías más frecuentes y costosas de incidentes cibernéticos. En segundo lugar, el desglose de costes operativos, reputacionales y legales asociado a estas brechas permite ilustrar con claridad el impacto empresarial que pueden tener este tipo de eventos. Muchas de las dinámicas recogidas en el informe de IBM —como los efectos reputacionales, la pérdida de clientes o el coste de contención y respuesta— son compartidas por otros ciberataques más allá de las filtraciones de datos, por lo que sus conclusiones pueden extrapolarse en parte al resto de casos analizados.

Según el informe, **los vectores de ataque más frecuentes en el entorno empresarial —y a la vez más costosos— son aquellos que aprovechan el factor humano y las brechas internas de seguridad**, como se muestra en la tabla 3.1.

Tipo de ataque	Frecuencia	Coste medio	Días hasta detección
Credenciales comprometidas	16 %	4,81M USD	292
Phishing	15 %	4,88M USD	261
Ransomware	8 %	4,91M USD	280
Insider malicioso	7 %	4,99M USD	308

Tabla 3.1: *Principales vectores de ataque por frecuencia e impacto. Fuente: IBM (2024).*

El uso de **credenciales comprometidas** representa el vector más común (16 %), y además uno de los más difíciles de detectar, con un promedio de *292 días* hasta su identificación y contención. Este tipo de ataque suele pasar desapercibido durante meses porque se produce dentro de canales aparentemente legítimos. Para las empresas, esto significa una exposición prolongada al robo de datos estratégicos, propiedad intelectual o información financiera sensible, con un coste medio de **4,81 millones de dólares**.

Le sigue de cerca el **phishing** o suplantación (15 %), una técnica que consiste en engañar a empleados para que entreguen información confidencial o accedan a enlaces maliciosos. El problema no es solo el acceso a la información, sino el daño a la reputación corporativa, especialmente si los clientes son víctimas indirectas del ataque.

El **ransomware** (8 %) representa una de las amenazas con mayor visibilidad mediática. Consiste en el cifrado de sistemas a cambio de un rescate económico. Su impacto es inmediato: paraliza completamente las operaciones, afecta la productividad y genera pérdidas tanto por interrupción del negocio como por costes de recuperación. El coste promedio de estos ataques se sitúa en **4,91 millones de dólares**, lo que lo convierte en uno de los más onerosos.

Finalmente, el **insider malicioso** (7 %) —un ataque perpetrado desde dentro de la organización, ya sea por un empleado o contratista— es el más costoso de todos: **4,99 millones de dólares** de media. Además, tiene el ciclo de detección más largo (*308 días*), ya que el atacante conoce los sistemas, procesos y debilidades internas. Para las empresas, esto no solo implica pérdidas económicas, sino también un serio problema de control interno y gobernanza corporativa.

Desde el punto de vista empresarial, estos datos dejan en evidencia varios aspectos críticos:

- **El factor humano sigue siendo la principal vulnerabilidad [41, 11]** en la mayoría de los casos, lo que pone de relieve la necesidad de invertir no solo en tecnología, sino también en formación, cultura organizativa y mecanismos de control interno.
- **La detección temprana es clave**: cuanto más tiempo tarda la empresa en identificar y contener una brecha, mayor es el impacto económico.

Por tanto, para una empresa, **gestionar adecuadamente el riesgo digital** ya no es una cuestión técnica delegable únicamente al departamento de TI, sino que **es una prioridad estratégica** que debe ser abordada desde la alta dirección, con impacto directo en la continuidad del negocio, la rentabilidad y el valor para los accionistas.

3.2 Estructura de costes y magnitud del impacto de un ciberataque

Por otro lado, si recordamos, el coste medio de una brecha de datos alcanzó los 4,88 millones de dólares en 2024 según el informe de IBM. Pero, ¿Cómo se reparte exactamente esta cifra dentro de la empresa afectada? ¿En qué áreas debe invertir una organización tras sufrir un incidente de este tipo?

En la tabla 3.2, podemos presenciar que, de esos 4,88 millones, la **mayor parte corresponde a las actividades de detección y contención** del incidente, **seguidas de cerca por la pérdida de negocio**, que refleja el impacto en la reputación y la continuidad operativa. **A continuación, se encuentran los costes asociados a la respuesta post-brecha**, que incluyen servicios legales y compensaciones a los afectados. **Por último, aunque en menor proporción, la notificación de la brecha supone un coste de 0,43 millones**, derivado de las obligaciones legales y regulatorias de informar tanto a los usuarios como a las autoridades pertinentes.

Este desglose evidencia cómo una brecha de seguridad no solo implica un problema técnico, sino que afecta a múltiples dimensiones del negocio, desde las operaciones hasta la confianza del cliente.

Categoría	Coste (M USD)	Componentes principales
Detección y contención	1,63	Investigación forense, auditorías de seguridad
Pérdida de negocio	1,47	Interrupción operativa, pérdida de clientes
Respuesta post-brecha	1,35	Servicios legales, monitorización de crédito
Notificación	0,43	Comunicación a afectados y reguladores
Total	**4,88**	

Tabla 3.2: *Desglose del coste promedio de una brecha de datos. Fuente: IBM (2024).*

3.3 Implicaciones estratégicas, regulatorias y sectoriales de ciberataques

Por otro lado, el impacto de los ciberataques no solo depende de su naturaleza técnica, sino también del sector económico en el que ocurren. Como puede verse en la figura 3.1, **el sector sanitario lidera con un coste promedio de 9,77 millones de dólares**, seguido por los servicios financieros (6,08M USD) y el sector farmacéutico (5,82M USD). Esta disparidad responde al valor intrínseco de los datos que manejan estos sectores en su actividad normal.

Frente a esta amenaza creciente, las organizaciones están incrementando su inversión en ciberseguridad. Sin embargo, **únicamente el 2 % de las empresas declara haber alcanzado un nivel completo de ciberresiliencia**, según una encuesta global de PwC [42].

Por último, cabe hacer especial mención al marco regulatorio, el cual también ha evolucionado para fomentar la transparencia y la rendición de cuentas en materia de ciberseguridad. En Estados Unidos, las *Data Breach Notification Laws* han obligado a las empresas a notificar públicamente cualquier incidente que afecte a datos personales, una línea también seguida en Europa mediante el Reglamento General de Protección de Datos (GDPR). Estas obligaciones legales no solo promueven mejores prácticas de protección de datos, sino que **amplifican las consecuencias reputacionales y financieras de los ciberincidentes**.

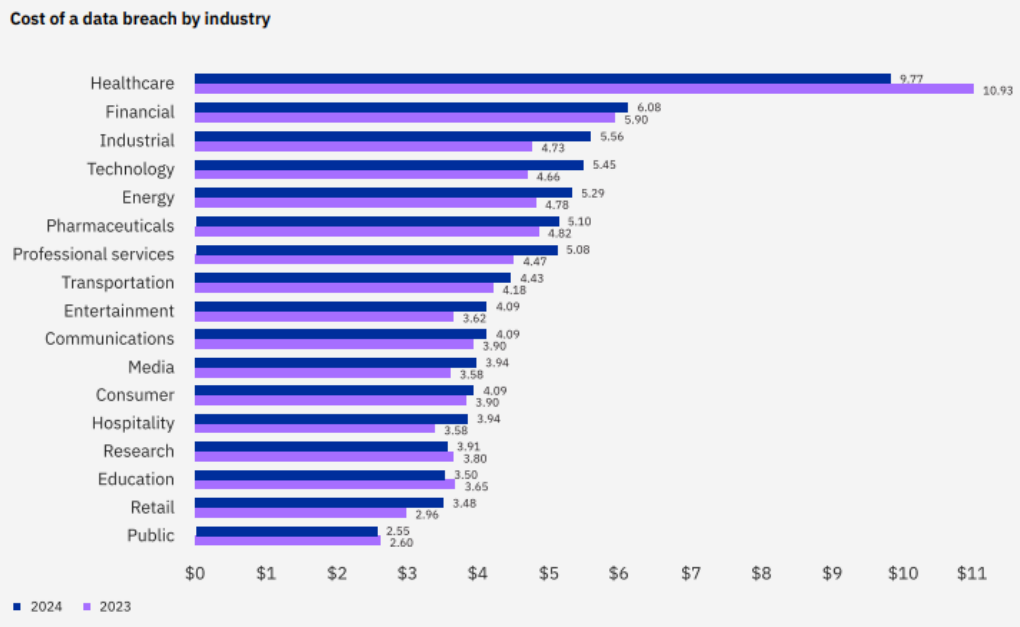

Figura 3.1: *Coste de una brecha de datos por sector empresarial. Fuente: IBM (2024)*

3.4 Contexto financiero y bursátil (2015–2025)

El comportamiento de los mercados bursátiles durante la última década es un factor clave para contextualizar el impacto de los ciberataques en empresas cotizadas. La reacción del mercado ante este tipo de eventos no solo depende del tipo de ataque o de la empresa afectada, sino también del entorno macroeconómico y financiero en el que ocurren.

Durante este periodo, el índice S&P 500 ha atravesado múltiples fases marcadas por una alta volatilidad estructural. Como se observa en la figura 3.2, entre 2012 y 2019 se registró una fase de crecimiento sostenido, impulsada por políticas monetarias expansivas. En 2020, la irrupción del COVID-19 provocó una caída abrupta superior al 30 %, seguida de una rápida recuperación gracias a los estímulos fiscales y monetarios implementados.

El bienio 2022–2023 estuvo dominado por una corrección del mercado, asociada a un entorno de inflación elevada, subidas de tipos de interés por parte de la Reserva Federal y tensiones geopolíticas como la guerra en Ucrania. A partir de 2023, se inició una nueva fase alcista, aunque altamente concentrada en un número reducido de compañías tecnológicas. El fenómeno conocido como *Magnificent 7* —que engloba a las principales firmas de IA y tecnología— llegó a explicar hasta el 84 % del crecimiento del Nasdaq 100 [43].

En 2025, el entorno continúa caracterizándose por una elevada incertidumbre y volatilidad, derivadas de tensiones comerciales entre Estados Unidos y otras potencias, así como por la creciente exposición tecnológica de las empresas. Este contexto refuerza la necesidad de analizar cómo eventos disruptivos como los ciberataques impactan la valoración de las empresas en tiempo real.

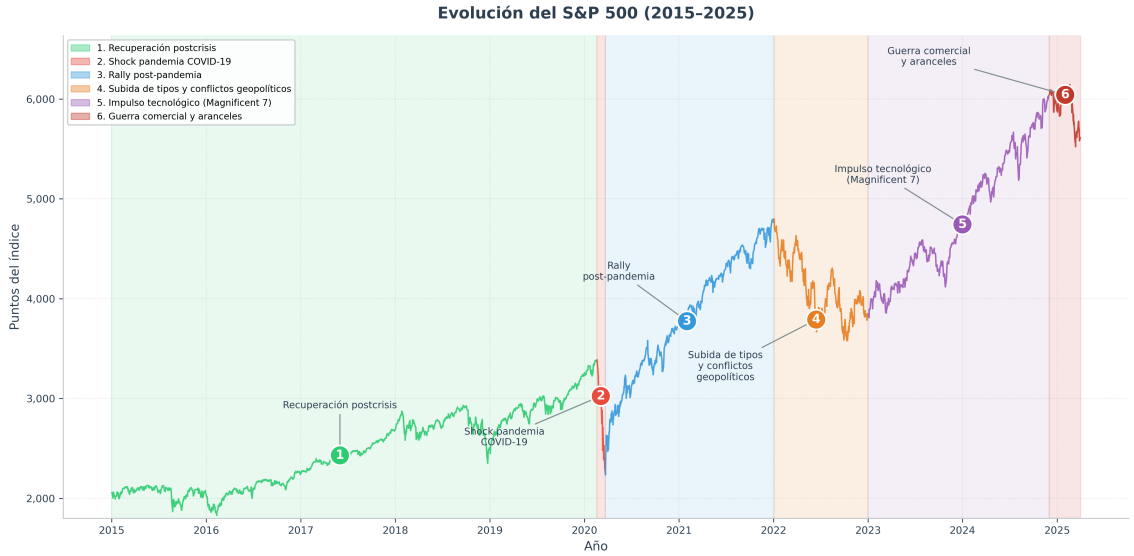

Figura 3.2: *Evolución del S&P 500 en relación con los eventos macroeconómicos y geopolíticos recientes. Fuente: Yahoo Finance (2025)*

En síntesis, lo que queda claro es que se ha establecido una dominancia clara de las empresas tecnológicas. Esta dominancia estructural del sector tecnológico en los mercados implica que cualquier incidente relevante —ya sea técnico o reputacional— puede generar efectos bursátiles a gran escala. En este contexto, estudiar el impacto de los ciberataques desde una perspectiva financiera y sectorial resulta no solo pertinente, sino necesario. Este será precisamente el objetivo del próximo capítulo.

CAPÍTULO 4
Metodología

Este capítulo presenta la estrategia metodológica empleada para cuantificar el impacto financiero de los ciberataques en empresas cotizadas. Partiendo del marco teórico establecido, se detalla la implementación práctica del estudio de eventos, desde la construcción de la muestra hasta el análisis estadístico de los resultados.

La metodología se estructura en torno a tres ejes fundamentales: el diseño de la muestra de eventos, el análisis de rentabilidad mediante retornos anormales y la evaluación de cambios en la percepción de riesgo a través de volatilidad. Cada una de estas dimensiones requiere decisiones metodológicas específicas que condicionan tanto la validez como la interpretabilidad de los hallazgos.

A diferencia del marco teórico, que establece los fundamentos conceptuales, vamos a hablar de las decisiones de implementación práctica: ¿Por qué seleccionar una ventana de estimación de 252 días? ¿Cómo garantizar que la fecha del evento es la correcta? ¿Qué criterios aplicar para construir un grupo de control válido? Estas elecciones van a determinar en gran medida la robustez y generalización de los resultados obtenidos.

A continuación, se presentan de manera secuencial las distintas etapas que han estructurado el trabajo.

4.1 Selección de la muestra

La construcción de una muestra rigurosa es esencial para garantizar la validez del análisis. La inclusión de eventos mal definidos o irrelevantes puede introducir sesgos y comprometer la calidad de los resultados. Para evitarlo, se aplicó un proceso de selección en dos fases: en primer lugar, se definieron los criterios metodológicos fundamentales; posteriormente, se implementaron filtros sistemáticos de inclusión.

Dado que los estudios de eventos exigen ciertas condiciones para asegurar la fiabilidad estadística, a continuación se presentan las principales consideraciones que guiaron el diseño de la muestra.

4.1.1. Consideraciones metodológicas para el estudio de eventos

- **Identificación precisa del momento del evento**: Es vital determinar cuándo exactamente la información se hace pública. En el caso de ciberataques, esto puede ser complejo debido a posibles desfases entre el incidente y su divulgación, o la existencia de filtraciones previas [28].

- **Tamaño muestral adecuado**: Estudios con pocas observaciones carecen de poder estadístico. Una muestra de al menos 20-30 eventos es generalmente considerada el mínimo para obtener inferencias confiables TEALL2023359.
- **Control de eventos confundentes**: Otros eventos simultáneos (anuncios de resultados, cambios directivos, noticias macroeconómicas) pueden contaminar la medición y deben ser identificados y controlados.

Una vez definidos los principios metodológicos, fue necesario traducirlos en una estrategia concreta de selección de casos que garantizara la validez del análisis. Para ello, se aplicaron los siguientes criterios, orientados a asegurar que cada evento cumpliese con los requisitos anteriormente expuestos:

a) **Horizonte temporal**: 2013–2024. Este periodo se seleccionó por ofrecer un equilibrio adecuado entre actualidad, disponibilidad de datos fiables y número suficiente de eventos relevantes.[1]

b) **Mercado**: emisores listados en NYSE o NASDAQ; se descartaron compañías que, a fecha del ataque, hubieran sido excluidas o absorbidas, ya que añadía una barrera innecesaria al proyecto encontrar los valores de cotización de las mismas. [2]

c) **Fecha única y verificable**: el ataque debía contar con un momento de *divulgación pública* **inequívoco** (p. ej. formulario 8-K[3], o nota de prensa de la propia organización). Se descartaron fuentes secundarias que pudieran citar la fecha de forma ambigua o incorrecta.

d) **Datos de mercado disponibles**: la serie histórica diaria de precios (valores de cierre ajustados) debía poder descargarse íntegramente a través de `yfinance`, tanto para la ventana de estimación como para la ventana del evento.

e) **Tamaño muestral mínimo**: se estableció como objetivo reunir al menos 20 eventos, umbral habitualmente aceptado en la literatura para garantizar resultados con validez estadística. Esta cifra permite equilibrar el rigor metodológico, el tiempo requerido para verificar la calidad de cada caso y la viabilidad operativa del análisis.

f) **Control de eventos confundentes**: se revisó manualmente que no coincidieran con el evento principal otras noticias relevantes que pudieran contaminar los resultados, como anuncios de resultados financieros, cambios en la dirección ejecutiva, operaciones corporativas o acontecimientos macroeconómicos. En los casos con posibles solapamientos, los eventos fueron descartados.

[1] El último incidente elegido se registró en 2024 para garantizar la disponibilidad de datos de cotización posteriores suficientes.

[2] Se seleccionaron únicamente empresas listadas en NYSE y NASDAQ debido a: (i) la transparencia y estricta regulación de divulgación impuesta por la SEC, que facilita identificar la fecha exacta de los eventos; (ii) la alta disponibilidad y calidad de datos históricos de cotización, accesibles mediante plataformas como `yfinance`; y (iii) la homogeneidad institucional que ofrece el mercado estadounidense, evitando sesgos derivados de marcos regulatorios diferentes.

[3] El Formulario 8-K es un informe que las empresas que cotizan en bolsa en Estados Unidos deben presentar ante la Securities and Exchange Commission (SEC) para notificar eventos relevantes que puedan afectar significativamente su situación financiera o el precio de sus acciones. Entre estos eventos se incluyen adquisiciones, cambios en la dirección, resultados financieros extraordinarios o incidentes de ciberseguridad.

4.1.2. Composición de la muestra

El proceso de filtrado dio como resultado una muestra final de 26 eventos, lo que permite realizar un análisis con suficiente poder estadístico sin comprometer el rigor metodológico. Para enriquecer el estudio, cada evento fue clasificado según tres dimensiones clave: sector económico, tipo de ataque y mercado de cotización. Esta categorización permite incorporar variables contextuales que podrían influir en la reacción del mercado y, al mismo tiempo, identificar patrones diferenciadores entre distintos tipos de empresas o incidentes.

- **Sector económico**: se clasificaron las empresas según su actividad principal (tecnología, sanidad, servicios financieros, etc.). Esta dimensión permite explorar si ciertos sectores, por su grado de digitalización, regulación o modelo de negocio, presentan una sensibilidad mayor frente a incidentes de ciberseguridad.
- **Tipología del ataque**: cada evento fue codificado según la naturaleza técnica del incidente. Se distinguió entre filtraciones de datos (*Data Breaches*) y ataques que afectan directamente a la operativa de la organización. Esta clasificación permite analizar si uno u otro tiende a provocar reacciones de mercado más intensas.
- **Mercado de cotización**: se distinguió entre empresas listadas en NYSE y NASDAQ, con el objetivo de comprobar si la reacción varía según el mercado en el que cotiza la empresa afectada.

4.2 Técnicas y herramientas utilizadas

El análisis se ha desarrollado utilizando herramientas de programación orientadas a la automatización de tareas críticas dentro del proceso de evaluación financiera. Este enfoque ha permitido una mayor eficiencia en el tratamiento de datos y ha reducido la posibilidad de errores humanos derivados de procedimientos manuales.

Todo el análisis se ha llevado a cabo mediante tres *scripts* desarrollados en Python (en su versión 3.13.3). Python es un lenguaje de programación ampliamente utilizado en el ámbito del análisis de datos, inteligencia artificial y, en el caso que nos ocupa, la economía aplicada. Además, se han utilizado diversas bibliotecas especializadas, cada una con funciones concretas que permiten abordar distintas fases del análisis:

- `pandas`: facilita la manipulación de bases de datos estructuradas (por ejemplo, series temporales de precios o rentabilidades), de forma similar a cómo se trabajarían en Excel, pero con mayor flexibilidad y eficiencia.
- `numpy`: se emplea para realizar cálculos matemáticos y operaciones vectorizadas, lo que permite manejar grandes volúmenes de datos de forma rápida.
- `matplotlib` y `seaborn`: permiten representar gráficamente los resultados, facilitando su interpretación y el análisis visual de patrones o relaciones entre variables.
- `statsmodels`: se utiliza para la estimación de modelos econométricos clásicos, como regresiones lineales o contrastes estadísticos, aplicables a problemas financieros.
- `arch`: permite trabajar con modelos de heterocedasticidad condicional (GARCH).
- `yfinance`: automatiza la descarga de datos bursátiles históricos directamente desde fuentes financieras confiables como Yahoo Finance, evitando la recopilación manual.

- `scikit-learn`: proporciona herramientas de modelización predictiva y análisis estadístico; en este caso, se ha utilizado para estimar el modelo CAPM mediante regresión lineal.

4.3 Implementación del estudio de eventos: análisis de la rentabilidad

Tras haber definido la muestra de eventos y detallado las herramientas estadísticas y computacionales empleadas, se procede a explicar cómo se ha implementado el análisis de rentabilidad basado en la metodología de estudios de eventos descrita en el capítulo anterior. Esta metodología permite **evaluar si los retornos de las acciones de empresas afectadas por un ciberataque difieren significativamente de los retornos esperados en ausencia de dicho evento**.

El Anexo B: *Código Python Utilizado* presenta una versión resumida del código, enfocada en los fragmentos esenciales utilizados para los análisis de rentabilidad y volatilidad.

El análisis de rentabilidad se estructura en las siguientes etapas:

1. **Obtención de datos históricos de precios:** se recopilan series temporales de precios diarios **tanto de las empresas afectadas** por cada evento **como del índice de referencia** utilizado como proxy del mercado.

   En este caso, se ha empleado el **S&P 500** (ticker `^GSPC`) como índice de referencia, dado que representa una muestra amplia y diversificada de 500 empresas de gran capitalización que cotizan en los principales mercados bursátiles estadounidenses (NYSE y NASDAQ).

   Su uso como benchmark está ampliamente aceptado en la literatura financiera [45], ya que refleja el comportamiento general del mercado y permite comparar de forma coherente los rendimientos de empresas individuales frente al conjunto del sistema financiero.

2. **Estimación del modelo CAPM:** Con los datos de cotización ya preparados calibramos el modelo CAPM de cada empresa mediante regresión para obtener los parámetros α_i y β_i. Empleamos una ventana de estimación de 252 días previos al evento. Esta ventana se eligió por representar un año completo de cotización [17, 29], proporcionando suficientes observaciones para una estimación robusta.

3. **Cálculo de los retornos anormales (AR)** como la diferencia entre los retornos observados y los retornos esperados que calculamos con el modelo CAPM a lo largo de la ventana del evento.

   Se analizaron cuatro horizontes temporales, para capturar tanto el impacto inmediato como su evolución a lo largo del tiempo:

   - **Ventana(-1, +1):** Captura la reacción inmediata del mercado
   - **Ventana(-2, +2):** Incluye posibles anticipaciones y ajustes posteriores
   - **Ventana(-5, +5):** Permite observar el comportamiento durante dos semanas bursátiles
   - **Ventana(-10, +10):** Evalúa la persistencia del impacto a medio plazo

4. **Cálculo del retorno anormal acumulado (CAR)** como la suma de los retornos anormales en cada ventana.

5. **Verificación de significancia estadística** mediante el test estadístico t y análisis del p-valor ($p - value$).
6. **Visualización de resultados**, y elaboración de gráficos resumen.

4.3.1. Pruebas de significancia para rendimientos anormales

Para determinar si las perturbaciones observadas son estadísticamente significativas o podrían deberse al azar, se aplicó el test t de Student. Este contraste evalúa si los retornos anormales acumulados (CAR) son significativamente distintos de cero, lo que indicaría que el ciberataque tuvo un impacto real en el valor de la empresa. Se utilizó un nivel de significancia del 5 %, estándar en estudios estadísticos.

- **Hipótesis nula (H_0)**: $\mu_{CAR} = 0$ El evento no afecta los rendimientos.
- **Hipótesis alternativa (H_1)**: El evento tiene efecto significativo en la rentabilidad.
- **Nivel de significancia**: 5 % ($\alpha = 0.05$).

El estadístico de prueba es:

$$t = \frac{C\bar{A}R}{s(CAR)/\sqrt{N}} \tag{4.1}$$

donde:

- $C\bar{A}R$: media muestral de los rendimientos anormales
- $s(CAR)$: desviación estándar muestral
- N: número de observaciones

Si $|t| > t_{\alpha/2, N-1}$ o si el p-valor es menor que el nivel de significancia, se rechaza la hipótesis nula y se concluye que el evento tuvo un impacto significativo en los rendimientos.

4.4 Implementación del estudio de eventos: análisis de la volatilidad

El análisis de volatilidad complementa el estudio de rentabilidad al examinar cómo los ciberataques afectan la percepción de riesgo del mercado. Mientras que el análisis de rentabilidad evalúa el impacto en los precios, el análisis de volatilidad cuantifica los cambios en la incertidumbre y el riesgo percibido por los inversores.

Para mantener la coherencia metodológica con el análisis de rentabilidad, **todos los cálculos de volatilidad se realizan sobre los residuos del modelo CAPM**, es decir, sobre los retornos anormales. Esta decisión metodológica permite aislar la volatilidad de la empresa, eliminando el componente de riesgo sistemático asociado al mercado.

El análisis de volatilidad se estructura en las siguientes etapas:

1. **Cálculo de residuos del CAPM para períodos pre y post evento:** Se utilizan los parámetros α y β estimados en el análisis de rentabilidad para calcular los retornos anormales (residuos) en dos períodos:

- **Período pre-evento:** 252 días bursátiles previos, excluyendo los 10 días inmediatamente anteriores al evento
- **Período post-evento:** 126 días bursátiles posteriores, comenzando 10 días después del evento

La exclusión de 20 días alrededor del evento evita que la volatilidad del período de crisis contamine la comparación de los niveles estructurales de riesgo. Para cada día t, el residuo se calcula como: $\varepsilon_t = R_t^{\text{empresa}} - (\alpha + \beta \times R_t^{\text{mercado}})$

2. **Cálculo de la volatilidad realizada de los residuos:** Se calcula la desviación estándar de los residuos del CAPM en ambos períodos, anualizada mediante el factor $\sqrt{252}$. Esta métrica representa la volatilidad anual del componente idiosincrático de los retornos.

3. **Test F de igualdad de varianzas sobre residuos:** Se aplica para determinar si el cambio en la volatilidad específica es estadísticamente significativo. El estadístico F compara directamente las varianzas de los residuos pre y post evento.

4. **Estimación del modelo GARCH(1,1) sobre residuos:** Para capturar la dinámica temporal de la volatilidad específica, se estima: $\sigma_t^2 = \omega + \alpha \cdot \varepsilon_{t-1}^2 + \beta \cdot \sigma_{t-1}^2$, donde ε_t son los residuos del CAPM.

5. **Análisis de persistencia del shock:** Se evalúa $\alpha + \beta$ para determinar la duración del impacto en la volatilidad específica.

6. **Validación mediante grupo de control:** Para confirmar que los cambios observados son atribuibles al ciberataque y no a movimientos generales del sector, se aplica la misma metodología a un grupo de control compuesto por empresas del mismo sector sin incidentes en el período analizado. Esta comparación permite aislar el efecto específico del evento.

4.4.1. Pruebas de significancia para cambios en volatilidad

Para determinar si los cambios observados en la volatilidad específica son estadísticamente significativos, se aplica el test F de Fisher para igualdad de varianzas. Este test es apropiado cuando se comparan varianzas entre dos muestras independientes de residuos.

- **Hipótesis nula (H_0)**: $\sigma^2_{\text{residuos,pre}} = \sigma^2_{\text{residuos,post}}$ (la volatilidad específica no cambia)
- **Hipótesis alternativa (H_1)**: $\sigma^2_{\text{residuos,post}} > \sigma^2_{\text{residuos,pre}}$ (existe cambio significativo)
- **Nivel de significancia**: 5 % ($\alpha = 0{,}05$)

El estadístico de prueba es:

$$F = \frac{\sigma^2_{\text{residuos,post}}}{\sigma^2_{\text{residuos,pre}}} \tag{4.2}$$

Si $F > F_{\alpha, n_2-1, n_1-1}$, se rechaza la hipótesis nula y se concluye que el ciberataque tuvo un impacto significativo en la volatilidad específica de la empresa.

4.4.2. Validación mediante grupo de control

Para confirmar que los cambios observados son atribuibles al ciberataque y no a movimientos generales del sector, se aplicó la misma metodología a un grupo de control compuesto por empresas del mismo sector sin incidentes en el período analizado. La comparación entre ambos grupos permite aislar el efecto específico del evento y verificar que no se debe a perturbaciones sistemáticas del mercado.

De la misma manera que en la elaboración de la muestra, la selección del grupo de control requirió la aplicación de criterios rigurosos para garantizar la comparabilidad. Para cada empresa afectada por un ciberataque, se identificó la empresa del mismo sector que presentara el mejor ajuste posible según los siguientes criterios:

1. **Clasificación sectorial**: Garantizando exposición a factores de riesgo sistemático similares.
2. **Capitalización bursátil comparable**: Se seleccionaron empresas cuya capitalización de mercado en el momento del evento se situara dentro del rango de $\pm 30\,\%$ respecto a la empresa afectada, minimizando sesgos derivados de diferencias de escala.
3. **Ausencia de eventos contaminantes**: Se verificó que las empresas de control no experimentaran eventos significativos durante la ventana del evento.
4. **Similitud en el modelo de negocio**: Empresas con modelos operativos y fuentes de ingresos comparables enfrentan riesgos empresariales similares.

Este proceso de emparejamiento permite establecer un contrafactual válido, es decir, una estimación creíble de cuál habría sido la evolución de la volatilidad de la empresa afectada en ausencia del ciberataque.

CAPÍTULO 5
Presentación de los resultados obtenidos

Una vez aplicada la metodología definida en el capítulo anterior, nos encontramos en disposición de presentar los resultados obtenidos. La presentación sigue una lógica progresiva, comenzando por una caracterización detallada de la muestra de eventos seleccionados, clasificados por sector económico, naturaleza del ataque y mercado de cotización.

A partir de esta base, se incluye un caso ilustrativo individual (Toyota) para mostrar paso a paso el proceso completo de análisis: desde la estimación del modelo de mercado, hasta el cálculo de los retornos anormales y el estudio de la volatilidad. Lo que se busca es ilustrar la aplicabilidad práctica del método antes de generalizar los resultados globales.

Seguidamente, se exponen los resultados agregados, tanto en términos de rentabilidad como de volatilidad. Asimismo, se analizan los efectos diferenciados según las características estructurales de las empresas afectadas. Finalmente, se incluye el análisis del grupo de control definido en la metodología, lo que permite contrastar la evolución de las empresas afectadas con la de sus pares no expuestos a ciberataques.

5.1 Análisis descriptivo de la muestra seleccionada

Tras aplicar la metodología de selección de ciberataques establecida en el capítulo anterior, se ha obtenido una muestra de 26 eventos. A continuación, se presentan en la tabla 5.1 algunos ejemplos representativos de los eventos que la componen:

Empresa	**Fecha**	**Descripción del ataque**
Equifax	2017-09-07	Violación de datos de 143 millones de personas; la acción cayó 35 % en el primer mes
Marriott	2018-11-30	Violación de datos de 500 millones de huéspedes en el sistema Starwood desde 2014
MGM Resorts	2023-09-10	Ataque de ransomware causó $100M en pérdidas y paralizó operaciones por 10 días
Capital One	2019-07-29	Violación de datos de 106 millones de clientes; hacker arrestada y multa de $80M

Tabla 5.1: *Resumen de eventos seleccionados para el análisis. Fuente: elaboración propia.*

El detalle completo de los 26 eventos, junto con las fuentes oficiales consultadas, se presenta en la tabla A.1 del Anexo A.

5.2 Composición de la muestra

Una vez definida la muestra, se consideró oportuno añadir algunas categorías que permitiesen buscar patrones diferenciadores ante eventos que iban a ser potencialmente distintos. A tal efecto, se han clasificado los eventos atendiendo a tres criterios: el sector económico al que pertenecen las empresas afectadas, el tipo de ataque sufrido y el mercado en el que cotizan.

5.2.1. Tipos de empresas

La primera dimensión considerada para clasificar las empresas afectadas ha sido su sector económico. Esta categorización permite evaluar si ciertos sectores, por su naturaleza digital, regulación o modelo de negocio, presentan mayor exposición o sensibilidad frente a incidentes de ciberseguridad.

Sector	**N.º de empresas**	**Ejemplos**
Tech & Telecommunications	11	Intel, Microsoft, Nvidia, CrowdStrike, Uber
Financial Services	3	Equifax, Capital One, JPMorgan Chase
Consumer & Services	8	Target, Clorox, Under Armour, MGM Resorts
Healthcare	4	UnitedHealth, 23andMe, Community Health Systems
Total	**26**	

Tabla 5.2: *Distribución de la muestra según el sector económico de las empresas afectadas. Fuente: elaboración propia.*

5.2.2. Tipologías de ataque

En segundo lugar, se ha clasificado cada evento según la naturaleza del ataque sufrido. Esta clasificación permite identificar si determinados patrones de ataque tienden a provocar reacciones más intensas por parte del mercado.

Tipología de ataque	**N.º de casos**	**Ejemplos**
Filtraciones de datos (*Data Breach*)	19	Equifax, Capital One, Snowflake
Ataques con impacto operativo	7	Clorox, CrowdStrike, UnitedHealth
Total	**26**	

Tabla 5.3: *Distribución de la muestra según el tipo de ataque sufrido. Fuente: elaboración propia.*

Nota: La mayoría de los eventos corresponden a filtraciones de datos, lo cual puede explicarse por la existencia de normativas de divulgación obligatoria (como el GDPR europeo o las leyes estatales en EE. UU.). Por su parte, los ataques con impacto operativo incluyen aquellos que interrumpen el funcionamiento de sistemas críticos, procesos logísticos o servicios esenciales.

5.2.3. Mercado de cotización

Por último, se ha tenido en cuenta el mercado bursátil en el que cotiza cada empresa.

Mercado bursátil	**N.º de empresas**	**Ejemplos**
NASDAQ	16	Facebook, CrowdStrike, T-Mobile
NYSE	10	Clorox, JPMorgan Chase, Toyota, Equifax
Total	**26**	

Tabla 5.4: *Distribución de la muestra según el mercado de cotización. Fuente: elaboración propia.*

5.3 Caso ilustrativo: Toyota

Para ilustrar el proceso completo del análisis, vamos a presentar el caso detallado de uno de los eventos. Más concretamente, el de Toyota (ticker: TM), que el 28 de febrero de 2022 reportó la suspensión de operaciones en 14 plantas en Japón, tras un ciberataque dirigido a su proveedor Kojima Industries, lo cual interrumpió temporalmente su cadena de suministro y paralizó 28 líneas de producción.

5.3.1. Estimación del modelo CAPM

Utilizando una ventana de estimación de 252 días previos al evento, se obtuvieron los siguientes parámetros del modelo CAPM:

- **Beta** = 0.6334, lo cual indica que Toyota presenta un perfil defensivo con respecto al mercado. Por cada 1 % de cambio en el S&P 500, el rendimiento esperado de Toyota se mueve un 0.63 %.

- **Alpha** = 0.000634, que representa el retorno medio diario de Toyota que no se explica por los movimientos del mercado.

- **R^2** = 0.1483. Aproximadamente el 15 % de la variabilidad de los retornos de Toyota viene explicada por el mercado (riesgo sistemático), el 85 % restante se debe a factores específicos de la empresa.

En la figura 5.1 se muestra la recta de regresión estimada, que representa gráficamente la relación entre las rentabilidades diarias de Toyota y del S&P 500 utilizada para estimar el modelo.

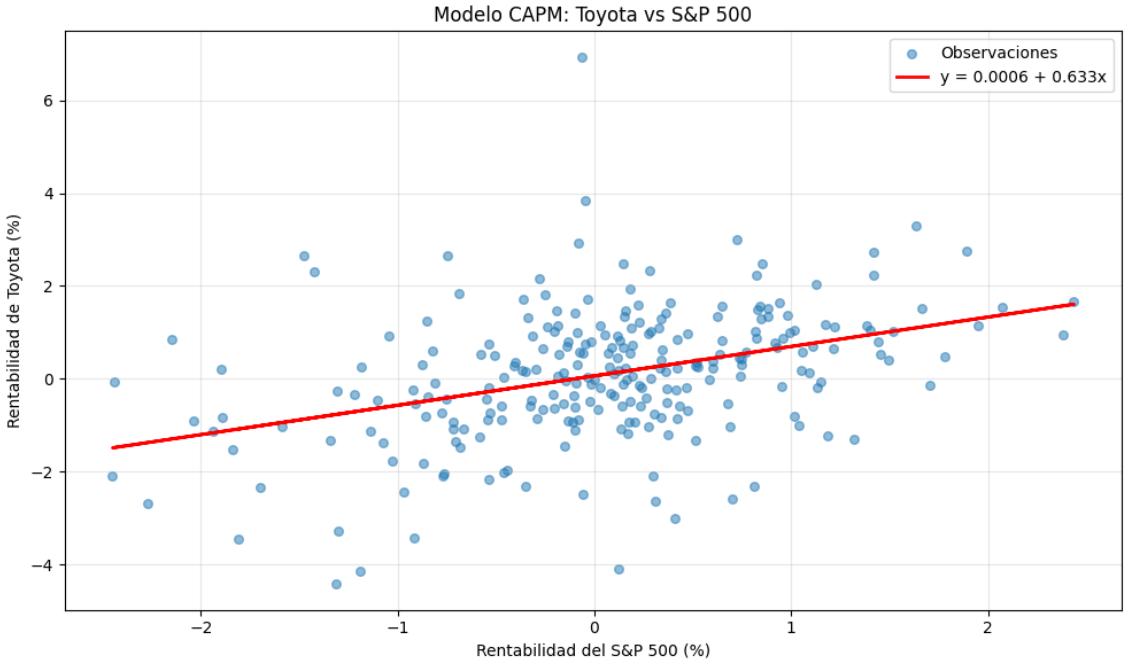

Figura 5.1: *Representación de la recta de regresión del modelo CAPM en el caso de Toyota. Fuente: elaboración propia*

Con estos parámetros ya obtenidos, los rendimientos esperados en ausencia del evento se calculan como:

$$\hat{R}_{\text{Toyota},t} = 0{,}0006 + 0{,}6334 \cdot R_{\text{Mercado},t}$$

Esta expresión representa el rendimiento teórico que habría obtenido la acción en cada día del período analizado, suponiendo que el evento no hubiera tenido lugar.

5.3.2. Cálculo de retornos anormales

Con los rendimientos esperados calculados, procedemos al cálculo de AR y CAR para cada ventana de evento. La tabla 5.5 muestra los resultados para la ventana [-5,+5]:

Día	R. Mercado	R. Esperado	R. Real	AR	CAR	Precio
-5	-0.72 %	-0.38 %	1.30 %	1.68 %	1.68 %	$174.50
-4	-1.01 %	-0.58 %	-1.76 %	-1.18 %	0.50 %	$171.42
-3	-1.84 %	-1.15 %	-0.97 %	0.18 %	0.68 %	$169.76
-2	1.50 %	1.13 %	-0.88 %	-2.01 %	-1.33 %	$168.27
-1	2.24 %	1.64 %	1.73 %	0.09 %	-1.24 %	$171.18
0	**-0.24 %**	**-0.06 %**	**-1.31 %**	**-1.25 %**	**-2.49 %**	**$168.94**
1	-1.55 %	-0.95 %	-0.68 %	0.27 %	-2.21 %	$167.79
2	1.86 %	1.38 %	-1.41 %	-2.79 %	-5.00 %	$165.43
3	-0.53 %	-0.25 %	-1.71 %	-1.46 %	-6.46 %	$162.60
4	-0.79 %	-0.43 %	-3.03 %	-2.60 %	-9.06 %	$157.67
5	-2.95 %	-1.91 %	-6.20 %	-4.29 %	-13.35 %	$147.90

Tabla 5.5: *Cálculo de retornos anormales (AR) y acumulados (CAR) para Toyota. Fuente: elaboración propia.*

Podemos ver cómo, al cierre del día +5, el precio de las acciones de Toyota había caído un 15.24 % respecto al día -5. Según el modelo CAPM, el 13.35 % de esta caída se considera un retorno anormal acumulado, es decir, una pérdida no explicada por el comportamiento general del mercado.

5.3.3. Prueba de significancia estadística

Una vez calculados AR y CAR, se procede a realizar el test t de Student. Su objetivo es evaluar si la media diaria de las rentabilidades anormales observadas durante la ventana del evento $[-5, +5]$ es estadísticamente distinta de cero. Concretamente, se calcula la media de los 11 ARs diarios de la ventana ($-1{,}21$ % diario, equivalente al CAR acumulado de $-13{,}35$ %) y se contrasta con el valor esperado bajo la hipótesis nula ($\overline{AR} = 0$, es decir, el ciberataque no tiene efecto sobre la rentabilidad).

La desviación estándar de esos mismos 11 ARs sirve para estimar la variabilidad natural de las rentabilidades anormales durante el período. Los resultados obtenidos son:

- Estadístico t: $-2{,}3078$
- Valor p: 0,0437

Dado que el valor $p < 0{,}05$, se rechaza la hipótesis nula con un nivel de confianza del 95 %. Por tanto, **se concluye que el evento analizado tuvo un impacto estadísticamente significativo en la rentabilidad de las acciones de Toyota durante la ventana del evento**.

Con el objetivo de evaluar la rapidez con la que el mercado incorporó la información relacionada con el incidente así como la posible reversión a lo largo del tiempo, se ha replicado el análisis estadístico sobre las ventanas definidas en la metodología: $(-1, +1)$, $(-2, +2)$ y $(-10, +10)$. Los resultados son:

Ventana	Estadístico t	Valor p	Significativo (5 %)
(-1, +1)	−0,5006	0,6663	No
(-2, +2)	−1,8292	0,1414	No
(-10, +10)	−1,7700	0,0920	No

Tabla 5.6: Resultados del test t para las ventanas complementarias del caso Toyota. Fuente: elaboración propia.

A la luz de estos resultados, se concluye que **el impacto negativo fue puntual y concentrado en el corto plazo**, alcanzando significancia estadística únicamente en la ventana $[-5, +5]$. Sin embargo, **no se observa un efecto estadísticamente significativo** en ventanas más cortas ($[-1, +1]$, $[-2, +2]$) ni más amplias ($[-10, +10]$), lo que sugiere que **el mercado no percibió el incidente como un evento con implicaciones estructurales duraderas**.

Para cerrar el análisis de los retornos de Toyota, la figura 5.2 presenta un resumen gráfico del estudio de eventos. Se muestran los retornos anormales diarios y acumulados, la comparación entre rentabilidad real y esperada, así como la evolución del precio de la acción en torno al evento. Esta visualización permite apreciar de forma clara el impacto bursátil del incidente.

5.3.4. Resumen gráfico estudio de eventos Toyota

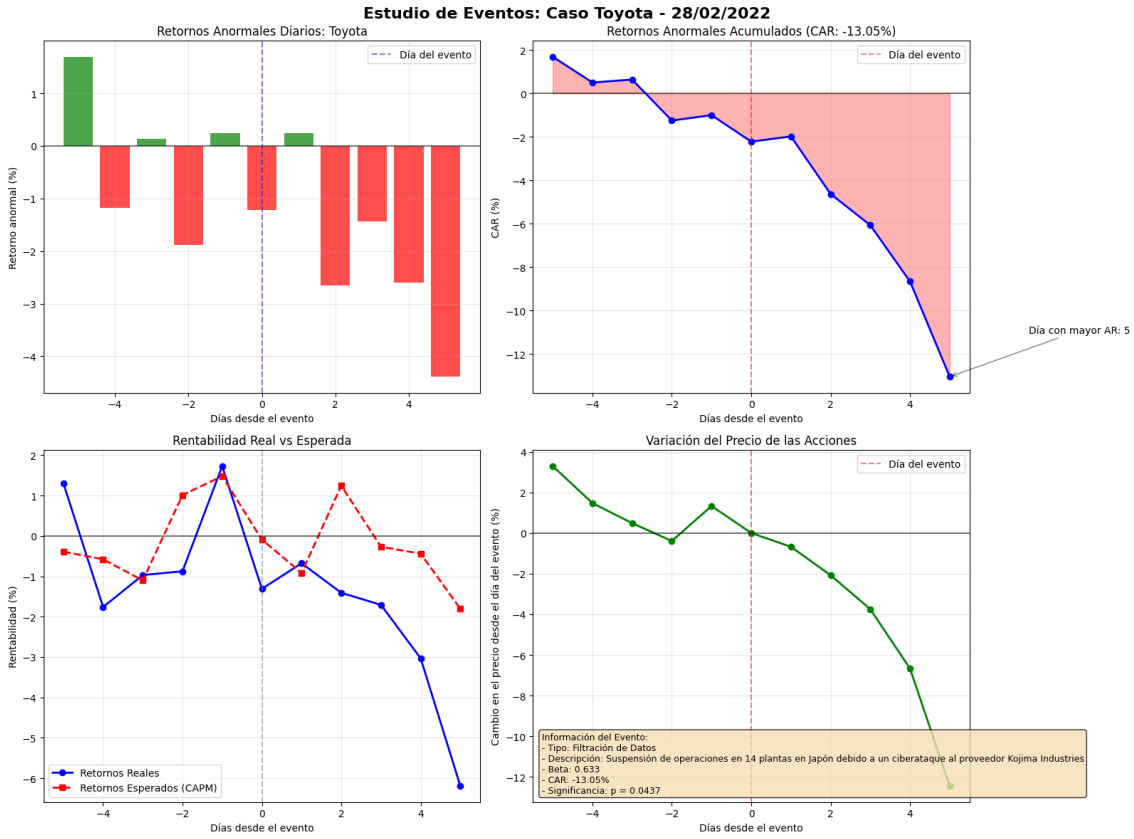

Figura 5.2: *Análisis completo de rentabilidad para Toyota mostrando el incremento post-evento. Fuente: elaboración propia*

5.3.5. Análisis de volatilidad

Tras analizar el impacto del ciberataque en los retornos, procedemos a examinar sus efectos sobre la volatilidad. Siguiendo la metodología establecida en la sección 4.3, el análisis se realiza sobre los residuos del modelo CAPM para aislar el riesgo específico de Toyota del riesgo sistemático del mercado.

Cálculo de la volatilidad específica

Los residuos del CAPM representan la componente de los retornos no explicada por los movimientos del mercado:

$$\varepsilon_t = R_{Toyota,t} - (\alpha + \beta \cdot R_{Mercado,t}) \tag{5.1}$$

donde $\alpha = 0{,}000634$ y $\beta = 0{,}6334$ eran los parámetros que habíamos estimado en el apartado de rentabilidad.

Se calculó la volatilidad anualizada de los residuos en dos períodos: 252 días pre-evento y 126 días post-evento (excluyendo 10 días alrededor del evento).

Métrica	Pre-evento	Post-evento	Cambio
Volatilidad anualizada (residuos)	20,79 %	20,42 %	−1,79 %
Varianza de residuos	0,000 172	0,000 165	−4,07 %
Test de hipótesis			
F-estadístico	0,965		–
p-valor	0,5815		No significativo

Tabla 5.7: *Análisis de volatilidad sobre residuos CAPM para Toyota. Fuente: elaboración propia.*

El test F de igualdad de varianzas no rechaza la hipótesis nula (p = 0.5815), indicando que **no existe un cambio estadísticamente significativo en la volatilidad específica** de Toyota.

La Figura 5.3 muestra la evolución de la volatilidad mediante una ventana móvil de 20 días:

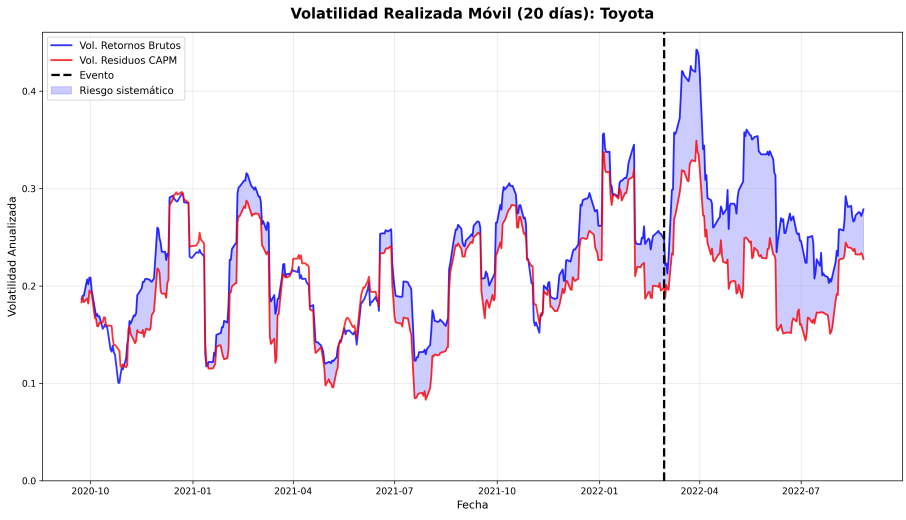

Figura 5.3: *Evolución de la volatilidad realizada. Fuente: elaboración propia.*

La gráfica revela que, aunque la volatilidad total aumentó tras el evento, este incremento se debe principalmente a una mayor volatilidad del mercado en general. Aunque en la fecha del evento tanto la volatilidad de los retornos brutos, como la de los residuos es similar, el incremento de la volatilidad específica de Toyota (línea roja) sigue una tendencia mucho menos pronunciada.

Modelo GARCH(1,1) sobre residuos

Para capturar la dinámica temporal, estimamos un modelo GARCH(1,1) sobre los residuos:

Período	α **(ARCH)**	β **(GARCH)**	**Persistencia** (α+β)
Pre-evento	0.0000	1.0000	1.0000
Post-evento	0.0000	0.9743	0.9743
Cambio	–	–	-2.57 %

Tabla 5.8: *Parámetros GARCH(1,1) estimados sobre residuos CAPM. Fuente: elaboración propia*

Los resultados del modelo GARCH(1,1) deben interpretarse con cautela en este caso. En el período pre-evento, el modelo estima una persistencia de 1,000 ($\alpha = 0{,}000$, $\beta = 1{,}000$), lo que corresponde a un proceso no estacionario en el que los shocks de volatilidad no se disipan. Este resultado puede reflejar limitaciones del modelo ante las condiciones específicas de la serie (elevada volatilidad del mercado en el período previo al evento, coincidente con las tensiones geopolíticas de 2021-2022). En el período post-evento, la persistencia se reduce a 0,974, un valor elevado pero estacionario, lo que sugiere que, si bien los shocks tardan considerablemente en disiparse, la volatilidad tiende eventualmente a revertir a su nivel de largo plazo.

Conclusiones sobre volatilidad

Como síntesis, podríamos concluir que el análisis de volatilidad revela que:

1. **No hay evidencia de cambio estructural en el riesgo específico**: El test F sobre residuos no es significativo (p=0.5815)
2. **La percepción inicial puede ser engañosa**: Mientras que la volatilidad total aumentó, esto se debió a factores de mercado, no al ciberataque per se.

Por tanto, aunque el ciberataque tuvo un impacto significativo en los **retornos** de Toyota (CAR de -13.35 %), no alteró fundamentalmente su **perfil de riesgo específico**. Esto sugiere que el mercado procesó el evento como una pérdida puntual más que como un cambio estructural en la incertidumbre futura de la empresa.

La presentación de los resultados de Toyota sirve como ejemplo ilustrativo del procedimiento aplicado sistemáticamente a cada uno de los 26 eventos analizados. A continuación, vamos a pasar a exponer los resultados globales del estudio, que permiten extraer conclusiones agregadas sobre el impacto de los ciberataques en los mercados financieros.

5.4 Presentación de los resultados globales

5.4.1. Análisis de la rentabilidad

Los hallazgos del análisis de rentabilidad para la muestra de 26 eventos se presentan de forma resumida en la Tabla 5.9. Dicha tabla detalla el Retorno Anormal Acumulado (CAR) y su correspondiente significancia estadística para cada evento a través de las diferentes ventanas temporales estudiadas. Para una consulta detallada de los parámetros del modelo CAPM y los p-valores, véase el Anexo C (Tablas C.1–C.4).

Evento	CAR (-1,1)	CAR (-2,2)	CAR (-5,5)	CAR (-10,10)
Target	0,004	−0,015	−0,026	−0,007
T-Mobile (2015)	−0,005	−0,042	−0,129**	−0,077
Equifax	−0,126	−0,215	−0,369	−0,358
Toyota	−0,007	−0,053	−0,131**	−0,148*
Clorox	−0,015	−0,032	−0,075**	0,033
Intel	−0,034*	0,000	−0,030	−0,244
Snowflake	−0,084	−0,113*	−0,199**	−0,275***
CrowdStrike	−0,278	−0,271	−0,331*	−0,531**
Sony	0,062*	0,031	0,051	0,042
Marriott	−0,036	−0,058	−0,044	−0,003
Facebook	−0,033	−0,033	−0,022	0,036
Capital One	−0,050	−0,029	0,015	0,004
Microsoft (2021)	−0,025*	0,005	−0,009	−0,048
T-Mobile (2021)	−0,026	−0,025	−0,009	−0,075
Microsoft (2022)	0,025	0,005	−0,009	−0,042
Nvidia	0,034	−0,021	0,001	0,023
Cisco	−0,011	−0,005	−0,016	0,050
Uber	0,047	0,058	0,050	0,074
MGM Resorts	−0,038	−0,051	−0,079	−0,141**
23andMe	−0,069**	−0,087	−0,159	−0,041
UnitedHealth	0,005	0,008*	−0,042	−0,073
Live Nation	0,006	−0,064	−0,025	−0,103
JPMorgan Chase	0,014	0,004	0,031	−0,005
eBay	−0,018	−0,008	−0,032	−0,031
Under Armour	−0,003	0,050	0,122	0,103
Community Health	0,001	0,021	0,038	0,099*
Media	**-0.033**	**-0.045**	**-0.065**	**-0.083**

Tabla 5.9: *Resumen de Retornos Anormales Acumulados (CAR) por evento y ventana. Fuente: elaboración propia.*

Nota: Los asteriscos indican el nivel de significancia estadística del CAR individual.
(***) p <0,01, (**) p <0,05, (*) p <0,10.

En la ventana inmediata de tres días $(-1, 1)$, 17 de los 26 eventos presentan un CAR negativo, de los cuales solo 2 son estadísticamente significativos. Sin embargo, a medida que se amplía el horizonte temporal, la media del CAR se va incrementando en valor absoluto. Esto sugiere que el mercado necesita varios días para procesar el impacto financiero de un ciberataque.

Completando el análisis, para evaluar si el impacto agregado es estadísticamente significativo, se aplicó un test t cross-sectional sobre la media de los CARs de los 26 eventos analizados. La hipótesis nula plantea que el CAAR medio es igual a cero ($H_0 : \overline{CAR} = 0$), frente a la alternativa de que existe un efecto significativo ($H_1 : \overline{CAR} \neq 0$). Los resultados se presentan en la Tabla 5.10.

Ventana	CAAR	t-stat	p-valor	Significativo
(± 1)	$-3{,}3$ %	$-1{,}802$	0,0841	No
(± 2)	$-4{,}5$ %	$-2{,}394$	0,0249	Sí**
(± 5)	$-6{,}5$ %	$-2{,}275$	0,0321	Sí**
(± 10)	$-8{,}3$ %	$-2{,}342$	0,0278	Sí**

Tabla 5.10: Test cross-sectional del CAAR por ventana de evento ($N = 26$). Fuente: elaboración propia.

Nota: (**) indica significancia estadística al 5 % ($p < 0{,}05$). El test evalúa si la media de los CARs individuales es significativamente distinta de cero.

Los resultados confirman que el CAAR es significativamente negativo al 5 % en las ventanas (± 2) ($t = -2{,}394$, $p = 0{,}025$), (± 5) ($t = -2{,}275$, $p = 0{,}032$) y (± 10) ($t = -2{,}342$, $p = 0{,}028$), mientras que en la ventana más corta (± 1) el efecto no alcanza significancia estadística ($t = -1{,}802$, $p = 0{,}084$). Confirmando así que, si bien la reacción inmediata del mercado (un solo día antes y después) no es concluyente por sí sola, el impacto acumulado a partir del segundo día es estadísticamente robusto y no atribuible al azar.

La figura 5.4 permite visualizar esta dinámica temporal día a día, representando el AAR (Retorno Anormal Medio) en forma de barras y el CAAR (Retorno Anormal Acumulado Medio) como una línea continua. En ella se pueden identificar tres hechos clave:

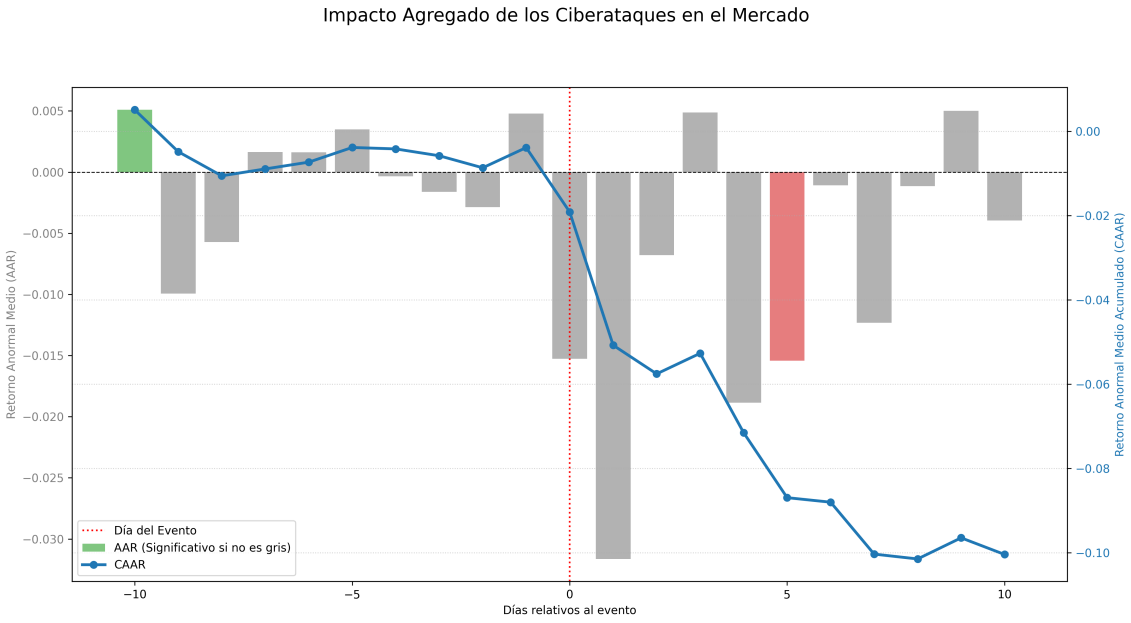

Figura 5.4: *Representación del AAR y CAAR de las empresas analizadas en la ventana (-10,10). Fuente elaboración propia*

- **Estabilidad pre-evento:** En el periodo previo al anuncio (días -10 a -1), el CAAR se mantiene estable y próximo a cero, validando la idoneidad del modelo, ya que el mercado no anticipa ningún evento en concreto.

- **Inicio de la reacción:** La curva del CAAR inicia un descenso pronunciado a partir del día 0, lo que confirma el impacto negativo inmediato del evento en el mercado.
- **Persistencia del impacto:** La reacción del mercado se extiende durante varios días. El Retorno Anormal Medio (AAR) diario registra su caída más pronunciada y estadísticamente significativa en el día +5.

Para concluir con el análisis de rentabilidad, vamos a hacer uso de las tres **variables categóricas** que habíamos definido en la muestra para realizar un análisis más detallado. Vamos a comenzar presentando los resultados obtenidos al analizar el sector empresarial; para ello, vamos a referirnos a la figura 5.5.

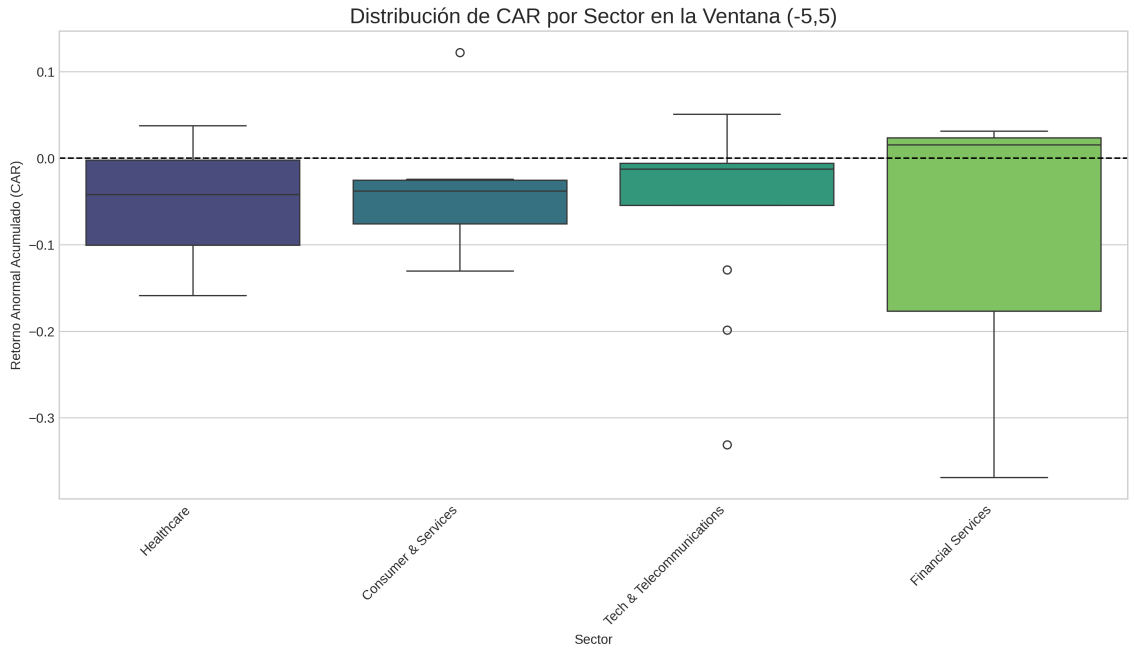

Figura 5.5: *Representación del impacto en el CAR por sector empresarial de las empresas analizadas. Fuente: elaboración propia*

Se observa que los sectores de Salud y Consumo y Servicios presentan el impacto negativo más consistente, con rangos intercuartílicos mayoritariamente por debajo de cero. Por su parte, el sector de Tecnología y Comunicaciones muestra una reacción más mixta: aunque su mediana es negativa, la distribución es más amplia y contiene varios outliers con CAR notablemente negativos. Finalmente, el sector de Servicios Financieros exhibe la mayor dispersión, con el rango más amplio de toda la muestra.

En cuanto al mercado de cotización (Figura 5.6), se aprecian diferencias notables en la distribución de los CARs. En el NASDAQ, la reacción del mercado es más consistentemente negativa, con una mediana situada en torno al -3 % y un rango intercuartílico que se encuentra casi en su totalidad por debajo de cero.

Por el contrario, la reacción en el NYSE es mucho más heterogénea. Si bien su mediana es muy similar, la principal diferencia radica en su mayor dispersión: los resultados abarcan desde reacciones positivas hasta el valor atípico más adverso de toda la muestra.

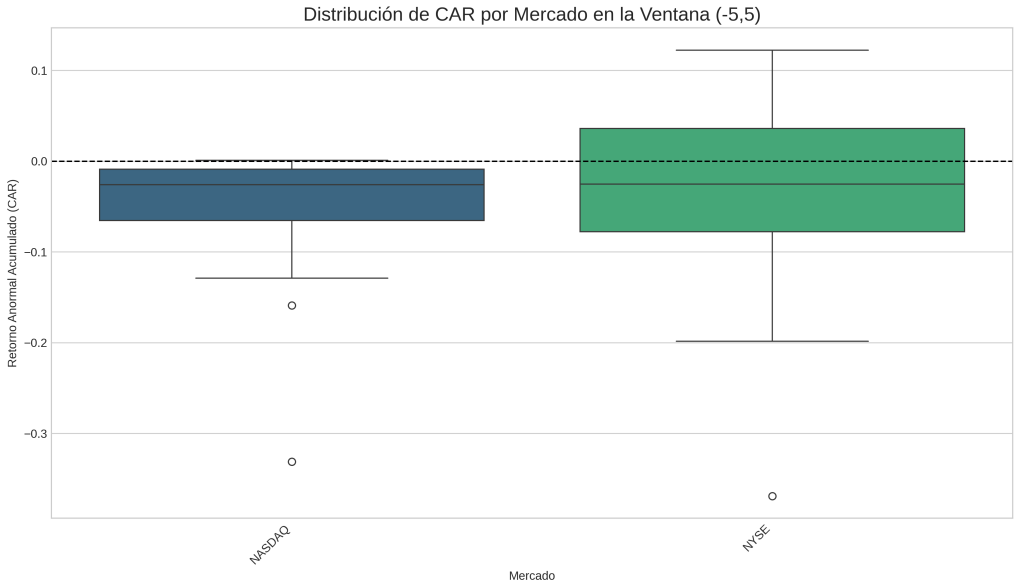

Figura 5.6: *Representación del impacto en el CAR por mercado de cotización de las empresas analizadas. Fuente: elaboración propia*

Por último, en cuanto al tipo de ataque (Figura 5.7), el mercado muestra una penalización más consistente y predecible para los Ataques a Sistemas y Operaciones. Como se observa en su diagrama de caja, el impacto es claramente negativo, con todo el rango intercuartílico situado por debajo de cero.

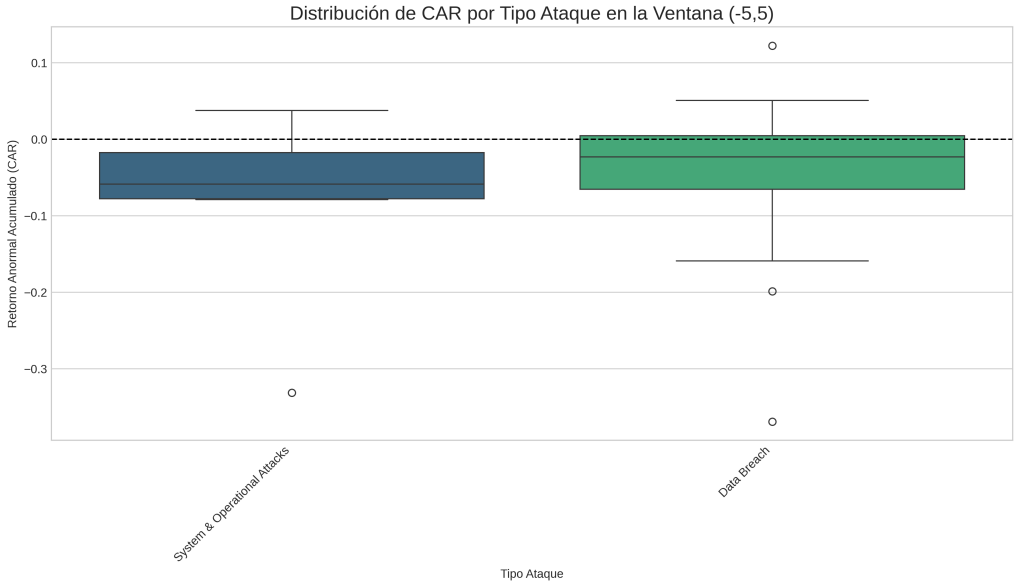

Figura 5.7: *Representación del impacto en el CAR por tipo de ataque. Fuente: elaboración propia*

En cambio, las filtraciones de datos, al igual que las empresas cotizadas en el NYSE, generan una reacción algo más variable. Si bien esta categoría incluye algunos de los eventos con peor rendimiento (que corresponderían con los valores atípicos), su mediana se sitúa más próxima a cero y la dispersión de resultados es considerablemente mayor, indicando que el mercado no castiga todas las brechas de datos de la misma manera.

5.4.2. Análisis de la volatilidad

Los resultados del Test F sobre los residuos del modelo CAPM indican que los ciberataques tienen un impacto notable en el riesgo percibido por el mercado. El hallazgo principal es que 9 de los 26 eventos (un $\tilde{35}$ %) presentan un cambio estadísticamente significativo en la volatilidad específica tras el incidente.

En todos los casos significativos, el estadístico F-Stat es superior a 1, lo que indica que dicho cambio se traduce en un aumento de la volatilidad. Los incrementos más marcados se observan en eventos como 23andMe, T-Mobile (2021), Snowflake y Sony.

Evento	F-Stat Vol Residuos	p-valor Vol Residuos	Sig. Vol
Target	**1.523**	**0.003**	**Sí**
T-Mobile (2015)	**1.713**	**0.000**	**Sí**
Equifax	**1.671**	**0.000**	**Sí**
Toyota	0,965	0,582	No
Clorox	1,077	0,312	No
Intel	**1.382**	**0.017**	**Sí**
Snowflake	**1.769**	**0.000**	**Sí**
CrowdStrike	0,776	0,941	No
Sony	**1.753**	**0.000**	**Sí**
Marriott	0,989	0,520	No
Facebook	1,051	0,370	No
Capital One	0,646	0,996	No
Microsoft (2021)	0,342	1,000	No
T-Mobile (2021)	**2.139**	**0.000**	**Sí**
Microsoft (2022)	1,257	0,068	No
Nvidia	0,951	0,618	No
Cisco	0,372	1,000	No
Uber	0,779	0,939	No
MGM Resorts	0,911	0,715	No
23andMe	**3.210**	**0.000**	**Sí**
UnitedHealth	**1.558**	**0.002**	**Sí**
Live Nation	0,758	0,957	No
JPMorgan Chase	0,774	0,943	No
eBay	1,095	0,273	No
Under Armour	0,610	0,999	No
Community Health	0,975	0,556	No

Tabla 5.11: *Análisis de Volatilidad Específica (Test F sobre residuos del CAPM). Fuente: elaboración propia*

El análisis de la persistencia de la volatilidad, estimada mediante el modelo GARCH (Tabla 5.12), muestra que en 15 de los 26 eventos analizados esta aumentó tras el incidente. No obstante, si se consideran únicamente los casos en los que la volatilidad realizada también presentó un incremento estadísticamente significativo, el número se reduce a 6. Entre ellos se encuentran los eventos de Target, T-Mobile (2015), Snowflake, Sony, T-Mobile (2021) y 23andMe, en los que se observa un refuerzo claro tanto del nivel como de la persistencia del riesgo tras el ataque.

	GARCH Pre			GARCH Post			
Evento	**α Pre**	**β Pre**	**Persistencia Pre**	**α Post**	**β Post**	**Persistencia Post**	**Cambio en Persistencia**
Target	0,111	0,000	0,111	0,075	0,560	0,635	Aumenta
T-Mobile (2015)	0,084	0,000	0,084	0,000	0,996	0,996	Aumenta
Equifax	0,091	0,846	0,937	0,042	0,862	0,904	Disminuye
Toyota	0,000	1,000	1,000	0,000	0,982	0,982	Disminuye
Clorox	0,332	0,329	0,661	0,872	0,009	0,881	Aumenta
Intel	0,575	0,425	1,000	0,337	0,663	1,000	Sin cambio
Snowflake	0,000	0,948	0,948	0,000	1,000	1,000	Aumenta
CrowdStrike	0,045	0,732	0,777	0,000	0,805	0,805	Aumenta
Sony	0,057	0,082	0,139	0,000	0,910	0,910	Aumenta
Marriott	0,133	0,743	0,876	0,118	0,000	0,118	Disminuye
Facebook	0,000	1,000	1,000	0,610	0,000	0,610	Disminuye
Capital One	0,023	0,000	0,023	0,507	0,325	0,832	Aumenta
Microsoft (2021)	0,000	0,994	0,994	0,000	0,971	0,971	Disminuye
T-Mobile (2021)	0,111	0,777	0,888	0,000	1,000	1,000	Aumenta
Microsoft (2022)	0,000	0,969	0,969	0,000	0,000	0,000	Disminuye
Nvidia	0,317	0,033	0,350	0,000	0,996	0,996	Aumenta
Cisco	0,512	0,197	0,709	0,201	0,698	0,899	Aumenta
Uber	0,322	0,115	0,437	0,115	0,846	0,961	Aumenta
MGM Resorts	0,048	0,000	0,048	0,000	0,912	0,912	Aumenta
23andMe	0,005	0,944	0,949	0,000	0,954	0,954	Aumenta
UnitedHealth	0,043	0,718	0,761	0,124	0,000	0,124	Disminuye
Live Nation	0,052	0,000	0,052	0,099	0,823	0,922	Aumenta
JPMorgan Chase	0,000	0,988	0,988	0,017	0,932	0,949	Disminuye
eBay	0,034	0,000	0,034	0,000	0,991	0,991	Aumenta
Under Armour	0,693	0,000	0,693	0,000	0,974	0,974	Aumenta
Community Health	0,000	0,992	0,992	0,066	0,708	0,774	Disminuye

Tabla 5.12: *Análisis de Volatilidad Condicional (Modelo GARCH). Fuente: elaboración propia.*

Al introducir nuevamente la dimensión sectorial (Figura 5.8), se observa que, mientras en el sector `Consumo y Servicios` la volatilidad específica disminuyó tras el evento (una reducción de aproximadamente 2 puntos porcentuales), el resto de los sectores registró aumentos. Este incremento fue especialmente pronunciado en el sector `Salud`, donde la volatilidad anualizada de los residuos del modelo CAPM aumentó en unos 16 puntos porcentuales, reflejando un cambio sustancial en el riesgo no sistemático.

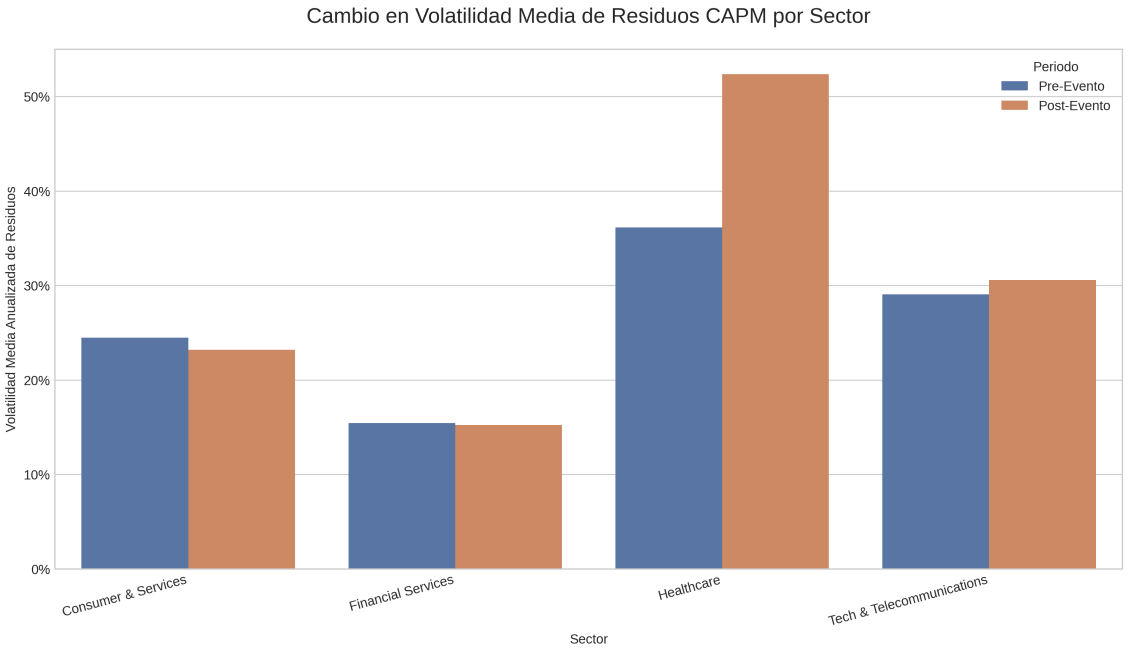

Figura 5.8: *Diagrama del cambio en la volatilidad realizada por sector. Fuente: elaboración propia.*

En cuanto al sector, en la figura 5.9 podemos ver que las empresas cotizadas en el NASDAQ han sido penalizadas en mayor medida en lo que a la volatilidad se refiere que las empresas del NYSE, con un incremento que es tres veces superior.

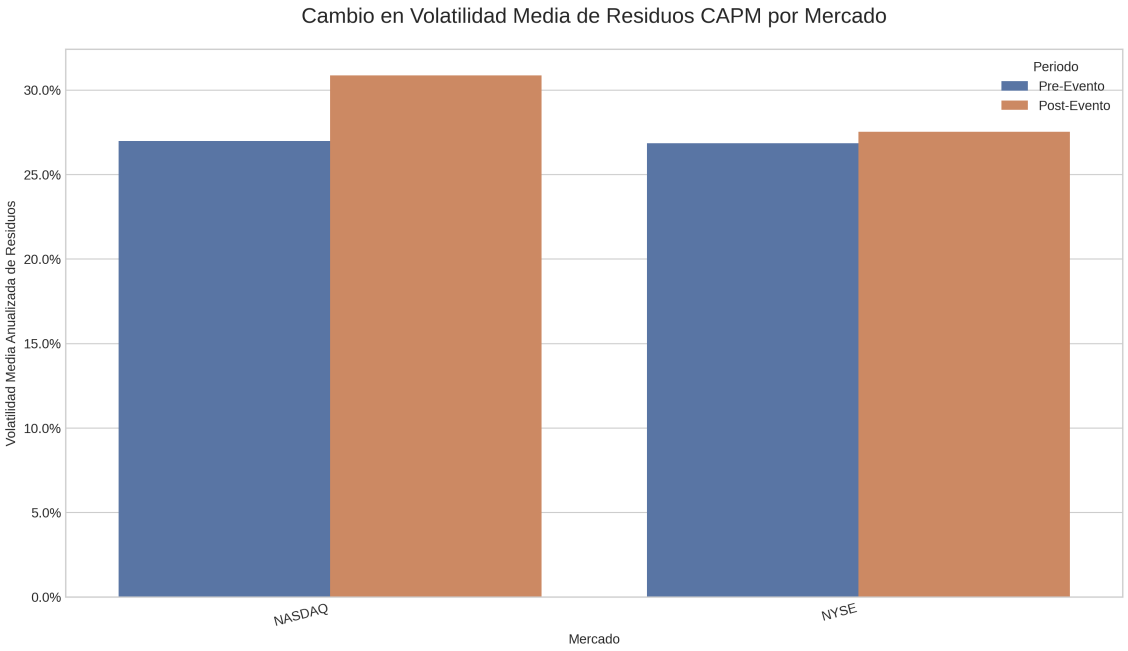

Figura 5.9: *Diagrama del cambio en la volatilidad realizada por mercado de cotización. Fuente: elaboración propia.*

Por último, al analizar los resultados según el tipo de ataque, como podemos ver en la figura 5.10 se observa que las empresas que han sufrido una brecha de datos han experimentado un aumento en su volatilidad. En contraste, los ataques vinculados a la cadena productiva han dado lugar a una disminución de la misma. Este hallazgo resulta particularmente relevante y será desarrollado en mayor profundidad en el siguiente capítulo.

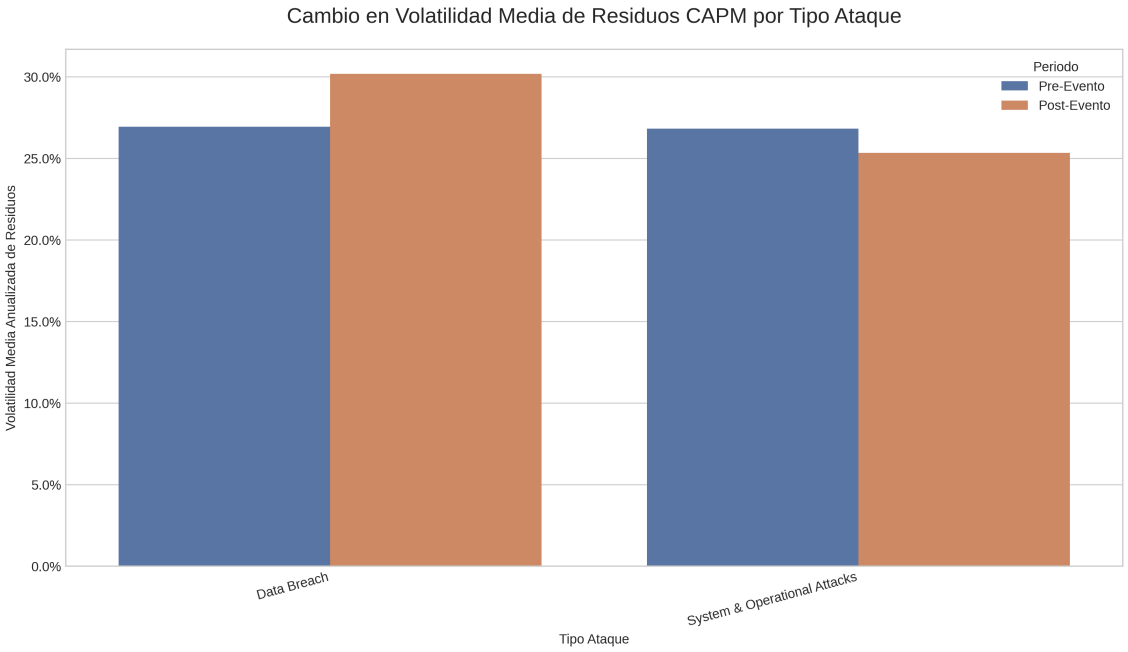

Figura 5.10: *Diagrama del cambio en la volatilidad realizada por tipo de ataque. Fuente: elaboración propia*

5.4.3. Comparación con empresas del grupo de control

Para cerrar la presentación de los resultados, es relevante comparar la evolución de la rentabilidad en las empresas que fueron objeto de ciberataques con la de un grupo de control compuesto por competidores directos que no sufrieron incidentes durante el mismo período. Esta comparación permite aislar el efecto específico del ataque, ayudando a determinar si fue realmente el causante de los efectos observados en las empresas afectadas.

Cada empresa de la muestra se emparejó con un competidor directo siguiendo los criterios de sector, capitalización y modelo de negocio descritos en la metodología. La composición detallada del grupo de control se encuentra en el Anexo D; a continuación, se presenta un ejemplo de los emparejamientos realizados:

Empresa Afectada	Empresa de Control	Justificación del Emparejamiento
Intel	AMD	Duopolio principal en el mercado de procesadores (CPU)

Tabla 5.13: *Ejemplos representativos de emparejamiento de la muestra y el grupo de control. Fuente: elaboración propia.*

Tras comparar ambos grupos, el gráfico 5.11 ofrece la evidencia visual más clara sobre la causalidad del impacto. En él se observa cómo, en el período previo al evento (días -10 a 0), tanto el grupo atacado como el de control siguen trayectorias similares.

Sin embargo, el día del anuncio del ciberataque marca un punto de inflexión bastante claro. A partir de ese momento, las dos líneas divergen de forma drástica: mientras el CAAR del grupo de control apenas varía, el del grupo afectado inicia una caída abrupta y sostenida, que alcanza una pérdida acumulada cercana al 10 % al final de la ventana. Esta notable diferencia de 6 puntos porcentuales entre ambos grupos aísla el efecto neto del incidente y confirma de manera robusta que los ciberataques provocan un impacto negativo y significativo en el valor de mercado de las empresas.

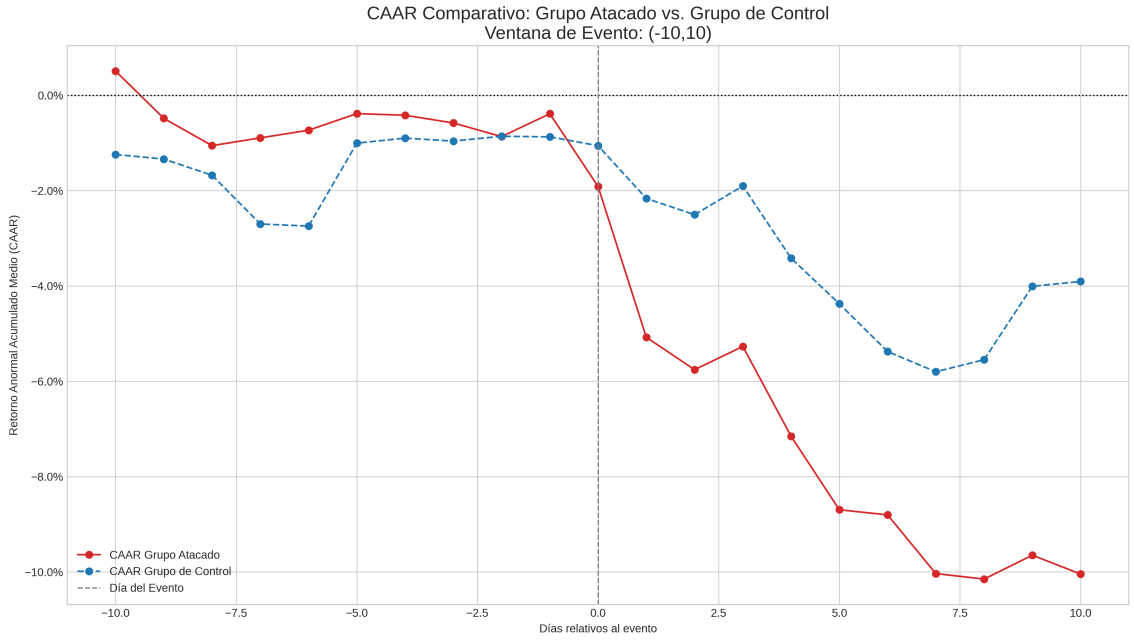

Figura 5.11: *Comparación de la evolución del CAAR entre empresas afectadas y de control. Fuente: elaboración propia.*

CAPÍTULO 6
Discusión de resultados

Con los resultados ya presentados, estamos en disposición de hacer una síntesis de los hallazgos más significativos, conectándolos con los objetivos de la investigación y la literatura existente, así como extraer sus implicaciones prácticas para empresas e inversores.

6.1 El impacto causal de los ciberataques en el valor de mercado

El hallazgo más relevante de este estudio es la confirmación de que **los ciberataques provocan una destrucción de valor estadísticamente significativa y directamente atribuible al incidente**. Como se mostró en la Figura 5.11, mientras que el CAAR del grupo afectado alcanzó el $-8{,}3$ % en la ventana (± 10), el grupo de control se mantuvo en torno al -2 %, lo que permite aislar un efecto neto de aproximadamente 6 puntos porcentuales atribuible exclusivamente al ciberataque.

Este comportamiento diferencial entre ambos grupos no solo valida la metodología empleada, sino que permite extraer tres conclusiones sobre la dinámica del impacto:

- **Ausencia de anticipación por parte del mercado.** Los retornos anormales acumulados en el periodo previo al evento se mantienen próximos a cero tanto en el grupo afectado como en el de control (Figura 5.11). Este resultado tiene una doble lectura: por un lado, respalda la hipótesis de eficiencia semifuerte [16] sobre la que se fundamenta el estudio, al confirmar que los precios no incorporan información sobre el ataque antes de su divulgación pública; por otro, refuerza la validez de la identificación de las fechas de evento, ya que una fecha incorrecta habría generado retornos anormales dispersos en el periodo previo.
- **Reacción inmediata pero prolongada.** El impacto negativo comienza el día del anuncio, pero lejos de ser un suceso puntual, la caída se acentúa durante la semana siguiente. El CAAR pasa del $-3{,}3$ % en la ventana (± 1) al $-8{,}3$ % en la ventana (± 10) (Tabla 5.10). Esto sugiere que el mercado no procesa la información de forma instantánea [44], sino que necesita varios días para valorar las consecuencias financieras, legales y reputacionales del incidente. Este patrón es consistente con la naturaleza compleja de los ciberataques, cuyo alcance real suele revelarse de forma progresiva a medida que avanzan las investigaciones forenses y se conocen nuevos detalles.

- **Incremento significativo del riesgo percibido.** La destrucción de valor no es el único efecto observable. Como se documentó en la Tabla 5.11, el 35 % de los eventos analizados presentó un aumento estadísticamente significativo de la volatilidad específica tras el incidente. Por tanto, la caída en el precio viene acompañada de un incremento en la percepción de incertidumbre por parte de los inversores, lo que podría traducirse en un mayor coste de capital [7] para la empresa afectada.

6.2 Factores que modulan la reacción del mercado

Si bien el efecto agregado es claramente negativo, el análisis por subcategorías revela que la magnitud y naturaleza de la reacción del mercado dependen de factores específicos que merecen una discusión detallada.

6.2.1. El tipo de ataque como factor diferenciador

Este es, probablemente, el hallazgo más relevante del análisis diferencial, puesto que revela un patrón aparentemente contradictorio en la forma en que el mercado procesa los distintos tipos de ciberataques.

Por un lado, los ataques a sistemas y operaciones generan una penalización en el precio más consistente y predecible, con todo el rango intercuartílico situado por debajo de cero (Figura 5.7). Esto se explica porque su impacto en el negocio es inmediato y cuantificable: la paralización de las plantas de Toyota supuso la interrupción de 28 líneas de producción, el ataque de ransomware a MGM Resorts generó pérdidas declaradas de 100 millones de dólares, y el incidente de Clorox provocó escasez de productos y pérdidas trimestrales significativas. En todos estos casos, el mercado puede estimar con relativa rapidez el coste del ataque en términos de ingresos perdidos.

Por otro lado, las filtraciones de datos, pese a incluir algunos de los eventos con mayor destrucción de valor (Equifax, Snowflake), presentan una dispersión considerablemente mayor en su CAR. Sin embargo, son precisamente estas filtraciones las que generan un mayor aumento de la volatilidad (Figura 5.10). Esta aparente contradicción tiene una explicación lógica: el coste final de una filtración de datos es inherentemente incierto en el corto plazo, ya que depende de factores que solo se conocerán semanas o meses después del incidente —como el alcance real de los datos comprometidos, las multas regulatorias, los litigios colectivos o la pérdida gradual de clientes—. Esta incertidumbre se traduce en una mayor volatilidad, mientras que la heterogeneidad en los precios refleja que el mercado evalúa cada filtración de forma muy diferente según su gravedad percibida.

6.2.2. La influencia del sector económico

El mercado penaliza con mayor severidad los ciberataques en sectores donde la confianza y la sensibilidad de los datos son críticas para el modelo de negocio. El sector sanitario presenta el impacto más adverso en ambas dimensiones: no solo registra un CAR consistentemente negativo (Figura 5.5), sino que además experimenta el mayor incremento de volatilidad de toda la muestra, con un aumento de aproximadamente 16 puntos porcentuales en la volatilidad anualizada de los residuos (Figura 5.8). Este resultado refleja la extrema sensibilidad de los datos médicos y genéticos, cuya exposición conlleva consecuencias regulatorias severas —especialmente bajo marcos como HIPAA en Estados Unidos— y un daño reputacional difícilmente reversible.

El sector de servicios financieros, por su parte, muestra la mayor dispersión en los CARs. Esta heterogeneidad podría explicarse por las diferencias en la magnitud de los incidentes dentro del sector: mientras que la filtración de Equifax (143 millones de registros) provocó una de las mayores caídas de la muestra, el ataque a JPMorgan Chase tuvo un impacto bursátil prácticamente nulo, posiblemente debido a la rápida respuesta de la entidad y a la percepción de solidez institucional por parte de los inversores.

6.2.3. La dinámica temporal del riesgo

El análisis GARCH aporta un matiz relevante sobre la naturaleza temporal del impacto en la percepción de riesgo. Aunque el 35 % de los eventos registró un aumento significativo en el nivel de volatilidad (Tabla 5.11), la persistencia de dicha volatilidad —medida por la suma $\alpha + \beta$— no siempre aumentó en la misma dirección. De los 26 eventos, 15 mostraron un incremento en la persistencia post-evento, pero los 11 restantes registraron una disminución (Tabla 5.12).

Este patrón sugiere que, en muchos casos, el mercado reacciona con un shock de volatilidad agudo pero transitorio: la incertidumbre se eleva bruscamente tras el anuncio del ataque, pero se disipa con relativa rapidez a medida que se conocen los detalles del incidente y la empresa comunica sus medidas de respuesta. No obstante, en los casos donde tanto el nivel como la persistencia aumentan simultáneamente —como ocurrió con 23andMe, T-Mobile (2021) o Snowflake—, el mercado señala un cambio más estructural en el perfil de riesgo de la empresa, lo que podría tener implicaciones duraderas para su coste de capital y su valoración.

6.3 Comparación con investigaciones previas

Los resultados de este trabajo son consistentes con la literatura que documenta la destrucción de valor asociada a los ciberataques. No obstante, la magnitud del impacto encontrado —un CAAR medio del $-6{,}84$ % en la ventana $(-10, +10)$— es notablemente superior al reportado en estudios previos: Cavusoglu et al. [18] documentaron un $-0{,}86$ %, Goel y Shawky [37] aproximadamente un -1 % y Celeny et al. [22] un $-1{,}3$ % para brechas de datos.

Esta divergencia puede explicarse por la confluencia de varios factores. En primer lugar, la **composición de la muestra**: mientras que los estudios citados se centran predominantemente en filtraciones de datos, este trabajo incluye también ataques con impacto operativo directo, que generan una penalización más severa. En segundo lugar, la **ventana temporal analizada** es más amplia (± 10 días frente a los ± 1 o ± 3 días habituales), lo que captura el efecto prolongado que otros estudios podrían no detectar. En tercer lugar, el **periodo muestral** (2013–2024) refleja un entorno de mayor dependencia digital y regulación más estricta, factores que podrían amplificar la reacción del mercado.

6.4 Implicaciones para empresas e inversores

Los hallazgos de este estudio tienen implicaciones prácticas directas:

1. **Para las empresas**: El coste de un ciberataque trasciende las partidas de gasto directo (reparación, multas) y se materializa en una destrucción significativa de valor bursátil. Este hallazgo redefine la forma en que debe justificarse la Inversión en Activos Fijos (CAPEX) en ciberseguridad. Dicha inversión deja de ser un mero coste

de TI para convertirse en una inversión estratégica cuantificable, cuyo retorno es la protección del valor para el accionista. Al demostrar que la inacción puede costar un gran porcentaje de la capitalización bursátil, este estudio proporciona una base sólida para que las empresas prioricen y aumenten su CAPEX en esta área. Además, la reacción prolongada del mercado subraya la necesidad de un plan de comunicación de crisis transparente y eficaz para gestionar la incertidumbre.

2. **Para los inversores**: El riesgo cibernético es un factor de riesgo financiero material y cuantificable que debería incorporarse en los modelos de valoración de activos. La postura de ciberseguridad de una empresa —entendida como su nivel de inversión, preparación y capacidad de respuesta ante incidentes— constituye un indicador relevante de la calidad de su gestión y debería formar parte del análisis fundamental previo a cualquier decisión de inversión. Además, el incremento de volatilidad documentado en el 35 % de los casos implica que los ciberataques no solo afectan al precio, sino que alteran el perfil de riesgo del activo, con implicaciones directas para la construcción y gestión de carteras.

CAPÍTULO 7
Propuestas de mejora

En este capítulo se exponen algunas propuestas de mejora y líneas de investigación futuras que podrían complementar y ampliar los hallazgos de este trabajo. Por limitaciones de tiempo y alcance del TFG, ciertas metodologías no fueron implementadas, pero constituyen extensiones naturales y de gran interés académico y práctico.

- **Uso de modelos de mercado más sofisticados.** Este estudio se ha basado en el modelo CAPM por su simplicidad y robustez. Investigaciones futuras podrían emplear modelos multifactoriales, como el de tres o cinco factores de Fama-French [31, 32], para controlar por otras fuentes de riesgo sistemático (como el tamaño de la empresa o su ratio valor contable/valor de mercado) y obtener así una estimación aún más precisa de los retornos anormales.

- **Ampliación de la muestra mediante extracción automatizada.** La muestra de 26 eventos se recopiló manualmente para garantizar la calidad y verificación de cada caso. Sin embargo, una muestra mayor aumentaría la potencia estadística de las conclusiones. Futuros trabajos podrían implementar técnicas de Procesamiento del Lenguaje Natural (NLP) para automatizar la extracción y clasificación de noticias sobre ciberataques de fuentes financieras, permitiendo analizar cientos de eventos y validar los patrones aquí encontrados a gran escala.

- **Análisis del impacto a largo plazo.** El estudio se centra en una ventana de 21 días. Una extensión natural sería analizar los efectos a medio y largo plazo (3, 6 y 12 meses) para determinar si la pérdida de valor es permanente o si las empresas tienden a recuperarse. Esto permitiría diferenciar entre un shock temporal y un daño estructural a la reputación y confianza de los inversores.

- **Segmentación por severidad del ataque y tamaño de la empresa.** La muestra podría segmentarse según la severidad del ataque (utilizando métricas como el número de registros filtrados) y el tamaño de la empresa. Esto permitiría responder a preguntas clave como: ¿castiga el mercado con más dureza los ataques de mayor envergadura? ¿Son las empresas más pequeñas, y potencialmente menos preparadas, más vulnerables a una pérdida de valor porcentual mayor? Esta segmentación se había contemplado en el proyecto, pero incluía la necesidad de establecer criterios para decidir cúando un ataque se encuadraría en una categoría u otra y no se disponía del tiempo suficiente para ello.

CAPÍTULO 8
Conclusiones

Este Trabajo de Fin de Grado tenía como objetivo principal cuantificar el impacto financiero de los incidentes de ciberseguridad en empresas cotizadas, analizando la reacción del mercado de valores ante su divulgación pública. Tras la aplicación de una metodología de estudio de eventos y el análisis de una muestra representativa de 26 ciberataques, se han obtenido conclusiones que no solo confirman las hipótesis iniciales, sino que también aportan nuevos matices sobre la relación entre la ciberseguridad y el valor corporativo.

8.1 Resumen de hallazgos clave

El hallazgo principal de esta investigación es inequívoco: los ciberataques provocan una destrucción de valor estadísticamente significativa y económicamente relevante para las empresas afectadas. Este impacto se manifiesta tanto en la rentabilidad como en el riesgo percibido por los inversores.

- **Impacto negativo y prolongado en la rentabilidad:** El análisis de los Retornos Anormales Acumulados (CAAR) revela una reacción negativa que comienza el mismo día del anuncio del ataque y se extiende durante al menos diez días hábiles posteriores. Este comportamiento sugiere que el mercado no solo penaliza el evento de forma inmediata, sino que tarda varios días en procesar y asimilar la totalidad de sus consecuencias financieras, operativas y reputacionales. La comparación con el grupo de control confirma que esta caída es atribuible directamente al ciberataque y no a movimientos generales del mercado.

- **Aumento significativo del riesgo percibido:** El análisis de volatilidad demuestra que los ciberataques alteran la percepción de riesgo de los inversores. En el 35 % de los casos analizados, la volatilidad realizada aumentó de forma estadísticamente significativa tras el incidente.

- **La naturaleza del ataque y el sector son determinantes:** No todos los ciberataques son iguales a ojos del mercado. Los ataques que afectan directamente a los sistemas y operaciones (como el *ransomware*) tienden a generar una penalización más consistente en el precio, mientras que las filtraciones de datos (*data breaches*) provocan un mayor aumento en la volatilidad. Del mismo modo, sectores como la Sanidad o los Servicios Financieros, donde la confianza y la sensibilidad de los datos son críticas, muestran una reacción más adversa.

8.2 Reflexiones finales e implicaciones

Los resultados de este estudio trascienden el ámbito puramente académico y ofrecen implicaciones prácticas de gran valor para la gestión empresarial y la toma de decisiones de inversión. La principal conclusión es la materialización del riesgo cibernético como un factor de riesgo financiero tangible y cuantificable, que ya no puede ser considerado un mero problema técnico del departamento de TI.

- **Para las empresas**, este trabajo proporciona una justificación económica para la inversión en ciberseguridad. Dicha inversión deja de ser un centro de coste para convertirse en una herramienta estratégica de protección del valor para el accionista.
- **Para los inversores y analistas financieros**, el estudio subraya la importancia de incorporar la evaluación de la postura de ciberseguridad de una empresa como parte integral de sus modelos de valoración y análisis de riesgos. La resiliencia digital de una compañía es un indicador de su calidad de gestión y de su capacidad para proteger sus activos intangibles, un factor cada vez más determinante en la economía actual.

En definitiva, en un entorno económico donde la digitalización es omnipresente, la capacidad de una organización para protegerse de las ciberamenazas está intrínsecamente ligada a su valor de mercado y a su viabilidad a largo plazo.

8.3 Líneas futuras de investigación

Partiendo de los hallazgos y limitaciones de este trabajo, se proponen las siguientes líneas de investigación futuras:

1. **Análisis a largo plazo:** Extender el horizonte de análisis a 6, 12 o 24 meses para determinar si la pérdida de valor es permanente o si las empresas logran recuperarse con el tiempo.
2. **Segmentación por severidad:** Analizar si la magnitud del impacto bursátil está correlacionada con métricas objetivas de la severidad del ataque, como el número de registros filtrados o el coste económico del rescate solicitado.
3. **Impacto de la respuesta de la empresa:** Investigar si la rapidez y transparencia de la comunicación de la empresa tras el ataque influyen en la reacción del mercado, premiando potencialmente a las organizaciones que gestionan la crisis de manera más eficaz.
4. **Extracción automatizada de eventos:** Utilizar técnicas de Procesamiento del Lenguaje Natural (NLP) para construir bases de datos de eventos de ciberseguridad a gran escala, permitiendo análisis más exhaustivos y la detección de patrones más sutiles.

Este trabajo ha aportado evidencia empírica sólida sobre el coste financiero de la vulnerabilidad digital. El camino a seguir implica profundizar en los factores que mitigan dicho coste, con el fin de construir un ecosistema empresarial más resiliente y seguro.

CAPÍTULO 9

Relación del trabajo con los objetivos de desarrollo sostenible (ODS)

A continuación, se detalla el grado de relación del presente Trabajo de Fin de Grado con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenible	**Alto**	**Medio**	**Bajo**	**No procede**
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**				X
ODS 4. **Educación de calidad.**			X	
ODS 5. **Igualdad de género.**				X
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**				X
ODS 8. **Trabajo decente y crecimiento económico.**	X			
ODS 9. **Industria, innovación e infraestructuras.**	X			
ODS 10. **Reducción de las desigualdades.**				X
ODS 11. **Ciudades y comunidades sostenibles.**				X
ODS 12. **Producción y consumo responsables.**			X	
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**		X		
ODS 17. **Alianzas para lograr objetivos.**			X	

Tabla 9.1: Grado de relación del TFG con los ODS.

9.1 Justificación de la Relación

9.1.1. Nivel de Relación: Alto

ODS 8: Trabajo decente y crecimiento económico Este TFG guarda una relación directa con este objetivo al cuantificar el impacto económico de los ciberataques sobre las empresas cotizadas. Los resultados muestran que los incidentes de ciberseguridad provocan caídas significativas en las cotizaciones bursátiles —con un CAR medio de hasta $-6{,}84\,\%$ en ventanas de ± 10 días— y aumentos de volatilidad en casi la mitad de los casos analizados. Estas pérdidas de valor afectan a accionistas, empleados y al tejido económico en general. El trabajo contribuye a concienciar sobre la necesidad de invertir en ciberseguridad como condición para un crecimiento económico sostenible y estable.

ODS 9: Industria, innovación e infraestructuras El análisis abarca empresas de sectores clave como tecnología, telecomunicaciones, servicios financieros y sanidad, cuya infraestructura digital es esencial para el funcionamiento de la economía moderna. Al evidenciar las consecuencias bursátiles de las brechas de seguridad, el trabajo subraya la importancia de construir infraestructuras digitales resilientes. Además, la propia metodología del estudio —combinando Event Study con modelos CAPM y análisis GARCH, implementados en Python— constituye un ejercicio de innovación aplicada a las finanzas.

9.1.2. Nivel de Relación: Medio

ODS 16: Paz, justicia e instituciones sólidas Los ciberataques estudiados —especialmente las brechas de datos que afectan a millones de usuarios— representan una amenaza a la confianza en las instituciones y a la protección de datos personales. El trabajo pone de manifiesto cómo el mercado penaliza a las empresas que no protegen adecuadamente la información de sus clientes, lo que refuerza la rendición de cuentas y la transparencia institucional. La ciberseguridad es, en última instancia, una cuestión de protección de derechos y de fortalecimiento de las instituciones.

9.1.3. Nivel de Relación: Bajo

ODS 4: Educación de calidad Como trabajo académico de fin de grado, el proyecto contribuye a la formación universitaria en finanzas cuantitativas y ciberseguridad corporativa, dos áreas de creciente relevancia profesional.

ODS 12: Producción y consumo responsables El estudio evidencia la responsabilidad que tienen las empresas en la custodia de los datos de sus consumidores. La reacción negativa del mercado ante las brechas de datos actúa como incentivo para que las organizaciones adopten prácticas más responsables en la gestión de la información.

ODS 17: Alianzas para lograr objetivos El trabajo se apoya en datos financieros públicos, herramientas de código abierto (Python, yfinance) y metodologías consolidadas en la literatura académica, promoviendo la colaboración y el conocimiento compartido en la comunidad científica.

Bibliografía

[1] BHARADWAJ, A.; EL SAWY, O.; PAVLOU, P.; y VENKATRAMAN, N. Digital Business Strategy: Toward a Next Generation of Insights. *MIS Quarterly*, 2013, 37(2): 471–482.

[2] DEHNING, B.; y RICHARDSON, V. Returns on Investments in Information Technology: A Research Synthesis. *Journal of Information Systems*, 2002, 16(1): 7–30.

[3] DAVENPORT, T. H. Putting the Enterprise into the Enterprise System. *Harvard Business Review*, 1998, 76(4): 121–131.

[4] JACOBS, F. R.; y WESTON, F. C. Enterprise Resource Planning (ERP)—A Brief History. *Journal of Operations Management*, 2007, 25(2): 357–363. DOI: https://doi.org/10.1016/j.jom.2006.11.002

[5] CHEN, H.; CHIANG, R. H. L.; y STOREY, V. C. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly*, 2012, 36(4): 1165–1188.

[6] VON SOLMS, R.; y VAN NIEKERK, J. From Information Security to Cyber Security. *Computers & Security*, 2013, 38: 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

[7] GORDON, L. A.; y LOEB, M. P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 2002, 5(4): 438–457. DOI: https://doi.org/10.1145/581271.581274

[8] BRUNDAGE, M.; AVIN, S.; CLARK, J.; TONER, H.; ECKERSLEY, P.; GARFINKEL, B.; y DAFOE, A. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation* [informe técnico en línea]. Future of Humanity Institute, University of Oxford, 2018. Disponible en: https://arxiv.org/abs/1802.07228

[9] BUCZAK, A. L.; y GUVEN, E. A Survey of Data Mining and Machine Learning Methods for Cybersecurity Intrusion Detection. *IEEE Communications Surveys & Tutorials*, 2016, 18(2): 1153–1176. DOI: https://doi.org/10.1109/COMST.2015.2494502

[10] SOMMER, R.; y PAXSON, V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. En: *IEEE Symposium on Security and Privacy*, pp. 305–316, 2010. DOI: https://doi.org/10.1109/SP.2010.25

[11] VERIZON. *2024 Data Breach Investigations Report* [en línea]. Nueva York: Verizon Business, 2024. Disponible en: https://www.verizon.com/business/resources/reports/dbir/

[12] KELLO, L. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, 2013, 38(2): 7–40. DOI: https://doi.org/10.1162/ISEC_a_00138

[13] WORLD ECONOMIC FORUM. *Global Cybersecurity Outlook 2025* [en línea]. Ginebra: World Economic Forum, enero 2025. Disponible en: https://www.weforum.org/publications/global-cybersecurity-outlook-2025

[14] IBM SECURITY. *Cost of a Data Breach Report 2024* [en línea]. Armonk (NY): IBM Corporation, julio 2024. Disponible en: https://www.ibm.com/reports/data-breach

[15] ROTHROCK, R. A.; KAPLAN, J.; y VAN DER OORD, F. The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review*, 2018, 59(2): 12–15.

[16] FAMA, E. F. Efficient Capital Markets: A Review of Theory and Empirical Work. *Journal of Finance*, 1970, 25(2): 383–417. DOI: https://doi.org/10.2307/2325486

[17] MACKINLAY, A. C. Event Studies in Economics and Finance. *Journal of Economic Literature*, 1997, 35(1): 13–39. Disponible en: https://www.jstor.org/stable/2729691 [Consulta: 3 ago 2025].

[18] CAVUSOGLU, H.; MISHRA, B.; y RAGHUNATHAN, S. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, 2004, 9(1): 70–104. DOI: https://doi.org/10.1080/10864415.2004.11044320

[19] SPANOS, G.; y ANGELIS, L. The Impact of Information Security Events to the Stock Market: A Systematic Literature Review. *Computers & Security*, 2016, 58: 216–229. DOI: https://doi.org/10.1016/j.cose.2015.12.006

[20] KAMIYA, S.; KANG, J.-K.; KIM, J.; MILIDONIS, A.; y STULZ, R. M. Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*, 2021, 139(3): 719–749. DOI: https://doi.org/10.1016/j.jfineco.2019.05.019

[21] MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA. *El Gobierno refuerza la ciberseguridad nacional con una inversión de más de 1 100 millones de euros* [nota de prensa en línea]. 6 may 2025. Disponible en: https://digital.gob.es/comunicacion/notas-prensa/mtdfp/2025/05/2025-05-06_02 [Consulta: 3 ago 2025].

[22] CELENY, A.; KURSHAN, S.; y WINTOKI, M. Cyberattacks and Stock Market Reactions: Evidence from Event Studies [preprint en línea]. *arXiv e-prints*, 8 feb 2024. Disponible en: https://arxiv.org/abs/2402.04773 [Consulta: 3 ago 2025].

[23] FAMA, E. F. Efficient Capital Markets II. *Journal of Finance*, 1991, 46(5): 1575–1617. DOI: https://doi.org/10.2307/2328565

[24] RITTER, J. R. The Buying and Selling Behavior of Individual Investors at the Turn of the Year. *Journal of Finance*, 1988, 43(3): 701–717. DOI: https://doi.org/10.2307/2328445

[25] BALL, R.; y BROWN, P. An Empirical Evaluation of Accounting Income Numbers. *Journal of Accounting Research*, 1968, 6(2): 159–178.

[26] FAMA, E. F.; FISHER, L.; JENSEN, M. C.; y ROLL, R. The Adjustment of Stock Prices to New Information. *International Economic Review*, 1969, 10(1): 1–21.

[27] KOTHARI, S. P.; y WARNER, J. B. Econometrics of Event Studies. En: ECKBO, B. E. (ed.), *Handbook of Empirical Corporate Finance*, vol. 1, pp. 3–36. Ámsterdam: Elsevier, 2007. DOI: https://doi.org/10.1016/B978-0-444-53265-7.50015-9

[28] TEALL, J. L. Capítulo 12 — Market Efficiency. En: *Financial Trading and Investing*, 3.ª ed., pp. 359–402. Londres: Academic Press, 2023. Disponible en: https://www.sciencedirect.com/science/article/pii/B9780323909556000124 [Consulta: 3 ago 2025].

[29] BROWN, S. J.; y WARNER, J. B. Using Daily Stock Returns: The Case of Event Studies. *Journal of Financial Economics*, 1985, 14(1): 3–31. DOI: https://doi.org/10.1016/0304-405X(85)90042-X

[30] SHARPE, W. F. Capital Asset Prices: A Theory of Market Equilibrium Under Conditions of Risk. *The Journal of Finance*, 1964, 19(3): 425–442. DOI: https://doi.org/10.2307/2977928

[31] FAMA, E. F.; y FRENCH, K. R. Common Risk Factors in the Returns on Stocks and Bonds. *Journal of Financial Economics*, 1993, 33(1): 3–56.

[32] FAMA, E. F.; y FRENCH, K. R. A Five-Factor Asset Pricing Model. *Journal of Financial Economics*, 2015, 116(1): 1–22. DOI: https://doi.org/10.1016/j.jfineco.2014.10.010

[33] TSAY, R. S. *Analysis of Financial Time Series*. 3.ª ed. Hoboken (NJ): Wiley, 2010.

[34] ENGLE, R. F. Autoregressive Conditional Heteroscedasticity with Estimates of the Variance of United Kingdom Inflation. *Econometrica*, 1982, 50(4): 987–1007. DOI: https://doi.org/10.2307/1912773

[35] ENGLE, R. F. GARCH 101: The Use of ARCH/GARCH Models in Applied Econometrics. *Journal of Economic Perspectives*, 2001, 15(4): 157–168. DOI: https://doi.org/10.1257/jep.15.4.157

[36] HOVAV, A.; y D'ARCY, J. The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, 2003, 6(2): 97–121. DOI: https://doi.org/10.1046/J.1098-1616.2003.026.x

[37] GOEL, S.; y SHAWKY, H. A. Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management*, 2009, 46(7): 404–410. DOI: https://doi.org/10.1016/j.im.2009.06.005

[38] KOLARI, J. W.; y PYNNÖNEN, S. Event Study Methodology: Correction for Cross-Sectional Correlation in Standardized Abnormal Returns. *Review of Financial Studies*, 2010, 23(11): 3996–4025.

[39] BRYNJOLFSSON, E.; y McAFEE, A. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*. Nueva York: W. W. Norton & Company, 2014.

[40] ZUBOFF, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Nueva York: PublicAffairs, 2019.

[41] PARSONS, K.; McCORMAC, A.; BUTAVICIUS, M.; PATTINSON, M.; y JERRAM, C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 2017, 42: 165–176. DOI: https://doi.org/10.1016/j.cose.2013.12.003

[42] PRICEWATERHOUSECOOPERS. *Encuesta Global de Confianza Digital 2025* [en línea], 2025. Disponible en: https://www.pwc.com/cl/es/Publicaciones/Encuesta-Global-de-Confianza-Digital-2025.html [Consulta: 3 ago 2025].

[43] YAHOO FINANCE. The Magnificent Seven Tech Stocks Drive Markets Higher as AI Mania Grips Investors [en línea]. 17 ene 2024. Disponible en: https://finance.yahoo.com/news/the-magnificent-seven-tech-stocks-drive-markets-higher-as-ai-mania-grips-investors-123029634.html [Consulta: 3 ago 2025].

[44] HONG, H.; y STEIN, J. C. A Unified Theory of Underreaction, Momentum Trading, and Overreaction in Asset Markets. *The Journal of Finance*, 1999, 54(6): 2143–2184. DOI: https://doi.org/10.1111/0022-1082.00184

[45] CAMPBELL, J. Y.; LO, A. W.; y MACKINLAY, A. C. *The Econometrics of Financial Markets*. Princeton (NJ): Princeton University Press, 1997.

[46] HUNTINGTON-KLEIN, N. Capítulo 17 — Event Studies. En: *The Effect: An Introduction to Research Design and Causality*. Princeton (NJ): Princeton University Press, 2023. Disponible en: https://theeffectbook.net/ch-EventStudies.html [Consulta: 3 ago 2025].

[47] HULL, J. C. *Options, Futures, and Other Derivatives*. 9.ª ed. Harlow: Pearson Education, 2015.

[48] MOORE, T. The Economics of Cybersecurity: Principles and Policy Options. *International Journal of Critical Infrastructure Protection*, 2010, 3(3–4): 103–117. DOI: https://doi.org/10.1016/j.ijcip.2010.10.002

[49] BOLLERSLEV, T. Generalized Autoregressive Conditional Heteroskedasticity. *Journal of Econometrics*, 1986, 31(3): 307–327. DOI: https://doi.org/10.1016/0304-4076(86)90063-1

[50] NELSON, D. B. Conditional Heteroskedasticity in Asset Returns: A New Approach. *Econometrica*, 1991, 59(2): 347–370. DOI: https://doi.org/10.2307/2938260

[51] CORBET, S.; y GURDGIEV, C. What the Hack: Systematic Risk Contagion from Cyber Events. *International Review of Financial Analysis*, 2019, 65: 101386. DOI: https://doi.org/10.1016/j.irfa.2019.101386

[52] TOSUN, O. K. Cyber-attacks and Stock Market Activity. *International Review of Financial Analysis*, 2021, 76: 101795. DOI: https://doi.org/10.1016/j.irfa.2021.101795

[53] FLORACKIS, C.; LOUCA, C.; MICHAELY, R.; y WEBER, M. Cybersecurity Risk. *The Review of Financial Studies*, 2023, 36(1): 351–407. DOI: https://doi.org/10.1093/rfs/hhac024

[54] FOERDERER, J.; y SCHUETZ, S. W. Data Breach Announcements and Stock Market Reactions: A Matter of Timing? *Management Science*, 2022, 68(10): 7298–7322. DOI: https://doi.org/10.1287/mnsc.2021.4187

APÉNDICE A

Apéndice A: Datos utilizados

Nombre empresa	Fecha	Descripción del ataque	Ref.
Target	2013-12-19	Violación de datos de 40 millones de tarjetas de crédito durante la temporada navideña.	[1]
T-Mobile	2015-10-01	Violación de datos de 15 millones de clientes a través de Experian.	[2]
Equifax	2017-09-07	Violación de datos de 143 millones de personas; la acción cayó 35 % en el primer mes.	[3]
Toyota	2022-02-28	Suspensión de operaciones en 14 plantas en Japón debido a un ciberataque al proveedor Kojima Industries, que interrumpió el sistema de suministro.	[4]
Clorox	2023-08-14	Ataque de ransomware que causó escasez de productos y pérdidas trimestrales significativas.	[5]
Intel	2020-08-06	Filtración de 20 GB de documentos internos y código fuente por un empleado.	[6]
Snowflake	2024-05-30	Campaña masiva comprometió datos de más de 100 clientes, incluidos AT&T y Santander.	[7]
CrowdStrike	2024-07-19	Actualización defectuosa causó apagón global que afectó aerolíneas, bancos y hospitales.	[8]
Sony	2014-11-24	Ataque atribuido a Corea del Norte filtró datos sensibles de empleados y correos electrónicos.	[9]
Marriott	2018-11-30	Violación de datos de 500 millones de huéspedes en el sistema Starwood desde 2014.	[10]
Facebook	2018-09-28	Violación de datos de 50 millones de usuarios por vulnerabilidad en «View As».	[11]
Capital One	2019-07-29	Violación de datos de 106 millones de clientes; hacker arrestada y multa de $80 M.	[12]
Microsoft	2021-03-02	250 000 servidores Exchange comprometidos por vulnerabilidad zero-day (HAFNIUM).	[13]
T-Mobile	2021-08-16	Violación de datos de 76.6 millones de personas; robo de SSN y licencias de conducir.	[14]
Microsoft	2022-01-18	Grupo Lapsus$ filtró código fuente de Bing, Cortana y otros productos.	[15]
Nvidia	2022-02-23	Lapsus$ robó ~1 TB de datos, incluidos esquemas de chips y credenciales de empleados.	[16]

Cisco	2022-08-05	Hackers accedieron a la red corporativa mediante ingeniería social y bypass de MFA.	[17]
Uber	2022-09-15	Adolescente obtuvo acceso interno mediante ingeniería social a un empleado.	[18]
MGM Resorts	2023-09-10	Ataque de ransomware causó $100 M en pérdidas y paralizó operaciones por 10 días.	[19]
23andMe	2023-10-01	Credential stuffing comprometió datos genéticos de 6.9 millones de usuarios.	[20]
UnitedHealth	2024-02-21	Ransomware a Change Healthcare impactó a un tercio de los estadounidenses; facturación médica paralizada.	[21]
Live Nation	2024-05-27	ShinyHunters robó datos de 560 millones de usuarios de Ticketmaster; pidieron rescate de $500 K.	[22]
JPMorgan Chase	2014-10-05	Violación de datos de 83 millones de cuentas (hogares y empresas).	[23]
eBay	2014-05-21	Violación que expuso datos de 145 millones de usuarios: nombres, direcciones, teléfonos y fechas de nacimiento.	[24]
Under Armour	2018-03-29	Violación de MyFitnessPal afectó a 150 millones de usuarios; hashes de contraseñas expuestos.	[25]
Community Health Systems	2014-08-18	APT chino robó datos de 4.5–6.1 millones de pacientes de 206 hospitales.	[26]

Tabla A.1: *Eventos seleccionados para la realización del estudio. Fuente: elaboración propia*

Referencias de la tabla

[1] https://www.sec.gov/Archives/edgar/data/27419/000110465914056760/a14-18360_1ex99.htm

[2] https://www.t-mobile.com/news/blog/experian-data-breach

[3] https://investor.equifax.com/news-events/press-releases/detail/240/equifax-announces-cybersecurity-incident-involving-consumer

[4] https://toyotatimes.jp/en/newscast/008.html

[5] https://www.sec.gov/Archives/edgar/data/21076/000120677423001133/clx4242401-8k.htm

[6] https://www.tomshardware.com/news/massive-20gb-intel-data-breach-floods-the-internet-mentions-backdoors

[7] https://snowflake.discourse.group/t/detecting-and-preventing-unauthorized-user-access/8967

[8] https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

[9] https://oag.ca.gov/system/files/12%2008%2014%20letter_0.pdf

[10] https://news.marriott.com/news/2018/11/30/marriott-announces-starwood-guest-reservation-database-security-incident

[11] https://about.fb.com/news/2018/09/security-update/

[12] https://www.capitalone.com/digital/facts2019/

[13] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[14] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation

[15] https://techcrunch.com/2022/03/23/microsoft-lapsus-hack-source-code/

[16] https://nvidia.custhelp.com/app/answers/detail/a_id/5333/

[17] https://blog.talosintelligence.com/recent-cyber-attack/

[18] https://www.uber.com/newsroom/security-update/

[19] https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

[20] https://blog.23andme.com/articles/addressing-data-security-concerns

[21] https://www.unitedhealthgroup.com/newsroom/2024/2024-04-22-uhg-updates-on-change-healthcare-cyberattack.html

[22] https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm

[23] https://www.sec.gov/Archives/edgar/data/19617/000119312514362173/d799478d8k.htm

[24] https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

[25] https://about.underarmour.com/en-us/stories/press-releases/release.12866.html

[26] https://www.sec.gov/Archives/edgar/data/1108109/000119312514126123/d705032d8k.htm

APÉNDICE B

Apéndice B: Código Python utilizado

```
class EnhancedEventStudy:
    def __init__(self, csv_path):
        self.data = pd.read_csv(csv_path)  # Leer archivo CSV con los eventos
        self.data['Fecha'] = pd.to_datetime(self.data['Fecha'])  # Convertir fechas a formato reconocible
```

Listing B.1: Carga de eventos desde archivo CSV

```
def get_market_data(self, market_ticker='^GSPC', start_date='2010-01-01'):
    # Definir la fecha maxima del evento mas 30 dias adicionales
    max_event_date = self.data['Fecha'].max() + timedelta(days=30)

    # Descargar los datos del indice S&P 500 desde Yahoo Finance
    market_data = yf.download(market_ticker, start=start_date, end=max_event_date)

    # Guardar en la clase para su uso posterior
    self.market_data = market_data
```

Listing B.2: Descarga de datos del mercado (S&P 500)

```
def get_event_window_data(self, ticker, event_date, estimation_window=252):
    # Calcular el rango de fechas: 252 dias habiles antes evento + margen
    start_date = event_date - timedelta(days=estimation_window + 50)
    end_date = event_date + timedelta(days=50)

    # Descargar los precios historicos desde Yahoo Finance
    stock_data = yf.download(ticker, start=start_date, end=end_date, progress=False)

    return stock_data
```

Listing B.3: Descarga de precios históricos para una acción individual

```
stock_data['Returns'] = stock_data['Close'].pct_change()
market_data['Returns'] = market_data['Close'].pct_change()
```

Listing B.4: Cálculo de rentabilidades diarias para la acción y el índice

```
# Extraer rendimientos del periodo de estimacion para Toyota
estimation_toyota = toyota_data['Returns'].iloc[estimation_start:
    estimation_end]

# Reindexar los datos del mercado para que coincidan con las fechas
     de Toyota
estimation_market = market_data['Returns'].reindex(
    estimation_toyota.index)
```

Listing B.5: Alineación de rendimientos de Toyota y del mercado

```
# Extraemos los retornos del mercado como variable independiente
X = aligned_data['market'].values.reshape(-1, 1)

# Extraemos los retornos de Toyota como variable dependiente (y)
y = aligned_data['toyota'].values

# Creamos y entrenamos el modelo de regresion lineal (CAPM)
model = LinearRegression()
model.fit(X, y)

# Obtenemos los parametros estimados: beta (pendiente) y alpha (
    intercepto)
beta = model.coef_[0]
alpha = model.intercept_

# Calculamos el coeficiente de determinacion R^2 del modelo
r_squared = model.score(X, y)
```

Listing B.6: Estimación de parámetros del modelo CAPM mediante regresión lineal

```
# Calcular AR (retornos anormales)
retornos_anormales = retornos_toyota_evento - retornos_esperados
```

Listing B.7: Cálculo de los retornos anormales (AR)

```
# Calcular CAR (retornos anormales acumulados)
retornos_anormales_acumulados = retornos_anormales.cumsum()
```

Listing B.8: Cálculo de los retornos anormales acumulados (CAR)

```
# Estadisticas de los retornos anormales
media_ar = retornos_anormales.mean()
std_ar = retornos_anormales.std()
n = len(retornos_anormales)

# Prueba t
t_estadistico = media_ar / (std_ar / np.sqrt(n))
p_valor = 2 * (1 - stats.t.cdf(abs(t_estadistico), n - 1))
```

Listing B.9: Cálculo del estadístico t y p-value para los retornos anormales

```
# Configuracion de la ventana movil para analisis de volatilidad
ventana_volatilidad = 20 # Establecemos la ventana movil que
    queramos analizar
volatilidad_movil = datos_toyota['Retornos'].rolling(window=
    ventana_volatilidad).std() * np.sqrt(252) # Calculamos la
    volatilidad para dicha ventana

print(f"Calculando volatilidad realizada con ventana movil de {
    ventana_volatilidad} dias...")
print("(Multiplicamos por sqrt(252) para anualizar la volatilidad)"
    )

# Definir periodos para comparacion
dias_comparacion = 30
pre_evento_inicio = max(0, idx_evento - dias_comparacion)
pre_evento_fin = idx_evento
post_evento_inicio = idx_evento
post_evento_fin = min(len(datos_toyota), idx_evento +
    dias_comparacion)

# Volatilidad promedio pre y post evento
vol_pre = volatilidad_movil.iloc[pre_evento_inicio:pre_evento_fin].
    mean()
vol_post = volatilidad_movil.iloc[post_evento_inicio:
    post_evento_fin].mean()
```

Listing B.10: Cálculo de volatilidad realizada y comparación pre/post evento

```
# Calcular estadistico F para comparar varianzas
var_pre = retornos_pre.var()  # Varianza de retornos pre-evento
var_post = retornos_post.var()  # Varianza de retornos post-evento
f_estadistico = var_post / var_pre  # Ratio de varianzas (F-
    estadistico)

# Grados de libertad para la distribucion F
df1 = len(retornos_post) - 1  # Grados de libertad del numerador
df2 = len(retornos_pre) - 1   # Grados de libertad del denominador

# Calculo del p-valor unilateral
# Si F > 1, buscamos P(F > f_estadistico)
# Si F < 1, buscamos P(F < f_estadistico)
if f_estadistico > 1:
    p_valor_vol = (1 - stats.f.cdf(f_estadistico, df1, df2))
```

Listing B.11: Prueba F para comparación de varianzas de retornos

```
from arch import arch_model

# Preparar datos para GARCH
inicio_garch = max(0, idx_evento - 504)  # 2 anyos antes
fin_garch = min(len(datos_toyota), idx_evento + 60)  # 60 dias
    despues

retornos_garch = datos_toyota['Retornos'].iloc[inicio_garch:
    fin_garch].dropna() * 100  # En porcentaje

# Ajustar modelo GARCH(1,1)
print("Estimando modelo GARCH(1,1)...")
modelo_garch = arch_model(retornos_garch, vol='Garch', p=1, q=1)
resultado_garch = modelo_garch.fit(disp='off')
persistencia = resultado_garch.params['alpha[1]'] + resultado_garch
    .params['beta[1]']
volatilidad_condicional = resultado_garch.conditional_volatility
```

Listing B.12: Estimacion del modelo GARCH(1,1) para volatilidad condicional

APÉNDICE C

Apéndice C: Resultados del análisis de rentabilidad y volatilidad

Evento	Fecha	Alpha	Beta	CAR (-1,1)	p-valor CAR	Sig. CAR
Target	2013-12-19	-0.000	0.553	0.004	0.931	No
T-Mobile	2015-10-01	0.001	0.836	-0.005	0.758	No
Equifax	2017-09-07	-0.000	1.006	-0.126	0.461	No
Toyota	2022-02-28	0.001	0.633	-0.007	0.666	No
Clorox	2023-08-14	0.000	0.474	-0.015	0.357	No
Intel	**2020-08-06**	**0.001**	**1.199**	**-0.034**	**0.013**	**Sí**
Snowflake	2024-05-30	-0.002	1.996	-0.084	0.187	No
CrowdStrike	2024-07-19	0.002	2.028	-0.278	0.148	No
Sony	2014-11-24	0.000	0.921	0.062	0.067	No
Marriott	2018-11-30	-0.000	1.021	-0.036	0.702	No
Facebook	2018-09-28	-0.001	1.335	-0.033	0.390	No
Capital One	2019-07-29	-0.000	1.079	-0.050	0.505	No
Microsoft	2021-03-02	0.001	1.112	-0.025	0.078	No
T-Mobile	2021-08-16	0.000	0.920	-0.026	0.532	No
Microsoft	2022-01-18	0.001	1.152	0.025	0.307	No
Nvidia	2022-02-23	0.001	2.222	0.034	0.319	No
Cisco	2022-08-05	-0.000	0.819	-0.011	0.289	No
Uber	2022-09-15	0.000	1.709	0.047	0.543	No
MGM Resorts	2023-09-10	0.001	1.312	-0.038	0.376	No
23andMe	**2023-10-01**	**-0.005**	**2.027**	**-0.069**	**0.031**	**Sí**
UnitedHealth	2024-02-21	0.000	0.220	0.005	0.256	No
Live Nation	2024-05-27	-0.000	1.115	0.006	0.836	No
JPMorgan Chase	2014-10-05	0.000	1.162	0.014	0.327	No
eBay	2014-05-21	-0.001	1.065	-0.018	0.212	No
Under Armour	2018-03-29	-0.001	1.413	-0.003	0.854	No
Community Health Systems	2014-08-18	-0.000	1.047	0.001	0.952	No
Total				-0.850		

Tabla C.1: Eventos y CAR para la ventana (-1,1)

Evento	Fecha	Alpha	Beta	CAR (-2,2)	p-valor CAR	Sig. CAR
Target	2013-12-19	-0.000	0.553	-0.015	0.705	No
T-Mobile	2015-10-01	0.001	0.836	-0.042	0.203	No
Equifax	2017-09-07	-0.000	1.006	-0.215	0.222	No
Toyota	2022-02-28	0.001	0.633	-0.053	0.141	No
Clorox	2023-08-14	0.000	0.474	-0.032	0.120	No
Intel	2020-08-06	0.001	1.199	-0.000	0.992	No
Snowflake	2024-05-30	-0.002	1.996	-0.113	0.097	No
CrowdStrike	2024-07-19	0.002	2.028	-0.271	0.172	No
Sony	2014-11-24	0.000	0.921	0.031	0.553	No
Marriott	2018-11-30	-0.000	1.021	-0.058	0.486	No
Facebook	2018-09-28	-0.001	1.335	-0.033	0.472	No
Capital One	2019-07-29	-0.000	1.079	-0.029	0.697	No
Microsoft	2021-03-02	0.001	1.112	0.005	0.877	No
T-Mobile	2021-08-16	0.000	0.920	-0.025	0.498	No
Microsoft	2022-01-18	0.001	1.152	0.005	0.903	No
Nvidia	2022-02-23	0.001	2.222	-0.021	0.717	No
Cisco	2022-08-05	-0.000	0.819	-0.005	0.703	No
Uber	2022-09-15	0.000	1.709	0.058	0.495	No
MGM Resorts	2023-09-10	0.001	1.312	-0.051	0.212	No
23andMe	2023-10-01	-0.005	2.027	-0.087	0.236	No
UnitedHealth	2024-02-21	0.000	0.220	0.008	0.054	No
Live Nation	2024-05-27	-0.000	1.115	-0.064	0.445	No
JPMorgan Chase	2014-10-05	0.000	1.162	0.004	0.828	No
eBay	2014-05-21	-0.001	1.065	-0.008	0.669	No
Under Armour	2018-03-29	-0.001	1.413	0.050	0.271	No
Community Health Systems	2014-08-18	-0.000	1.047	0.021	0.451	No
Total				-1.171		

Tabla C.2: Eventos y CAR para la ventana (-2,2)

Evento	Fecha	Alpha	Beta	CAR (-5,5)	p-valor CAR	Sig. CAR
Target	2013-12-19	-0.000	0.553	-0.026	0.509	No
T-Mobile	**2015-10-01**	**0.001**	**0.836**	**-0.129**	**0.012**	**Sí**
Equifax	2017-09-07	-0.000	1.006	-0.369	0.098	No
Toyota	**2022-02-28**	**0.001**	**0.633**	**-0.131**	**0.044**	**Sí**
Clorox	**2023-08-14**	**0.000**	**0.474**	**-0.075**	**0.046**	**Sí**
Intel	2020-08-06	0.001	1.199	-0.030	0.466	No
Snowflake	**2024-05-30**	**-0.002**	**1.996**	**-0.199**	**0.019**	**Sí**
CrowdStrike	2024-07-19	0.002	2.028	-0.331	0.088	No
Sony	2014-11-24	0.000	0.921	0.051	0.517	No
Marriott	2018-11-30	-0.000	1.021	-0.044	0.586	No
Facebook	2018-09-28	-0.001	1.335	-0.022	0.700	No
Capital One	2019-07-29	-0.000	1.079	0.015	0.842	No
Microsoft	2021-03-02	0.001	1.112	-0.009	0.804	No
T-Mobile	2021-08-16	0.000	0.920	-0.009	0.818	No
Microsoft	2022-01-18	0.001	1.152	-0.009	0.832	No
Nvidia	2022-02-23	0.001	2.222	0.001	0.993	No
Cisco	2022-08-05	-0.000	0.819	-0.016	0.480	No
Uber	2022-09-15	0.000	1.709	0.050	0.607	No
MGM Resorts	2023-09-10	0.001	1.312	-0.079	0.130	No
23andMe	2023-10-01	-0.005	2.027	-0.159	0.314	No
UnitedHealth	2024-02-21	0.000	0.220	-0.042	0.292	No
Live Nation	2024-05-27	-0.000	1.115	-0.025	0.783	No
JPMorgan Chase	2014-10-05	0.000	1.162	0.031	0.161	No
eBay	2014-05-21	-0.001	1.065	-0.032	0.377	No
Under Armour	2018-03-29	-0.001	1.413	0.122	0.142	No
Community Health Systems	2014-08-18	-0.000	1.047	0.038	0.366	No
Total				-1.701		

Tabla C.3: Eventos y CAR para la ventana (-5,5)

Evento	Fecha	Alpha	Beta	CAR (-10,10)	p-valor CAR	Sig. CAR
Target	2013-12-19	-0.000	0.553	-0.007	0.877	No
T-Mobile	2015-10-01	0.001	0.836	-0.077	0.285	No
Equifax	2017-09-07	-0.000	1.006	-0.358	0.120	No
Toyota	2022-02-28	0.001	0.633	-0.148	0.092	No
Clorox	2023-08-14	0.000	0.474	0.033	0.759	No
Intel	2020-08-06	0.001	1.199	-0.244	0.151	No
Snowflake	**2024-05-30**	**-0.002**	**1.996**	**-0.275**	**0.009**	**Sí**
CrowdStrike	**2024-07-19**	**0.002**	**2.028**	**-0.531**	**0.015**	**Sí**
Sony	2014-11-24	0.000	0.921	0.042	0.678	No
Marriott	2018-11-30	-0.000	1.021	-0.003	0.968	No
Facebook	2018-09-28	-0.001	1.335	0.036	0.629	No
Capital One	2019-07-29	-0.000	1.079	0.004	0.965	No
Microsoft	2021-03-02	0.001	1.112	-0.048	0.332	No
T-Mobile	2021-08-16	0.000	0.920	-0.075	0.114	No
Microsoft	2022-01-18	0.001	1.152	-0.042	0.510	No
Nvidia	2022-02-23	0.001	2.222	0.023	0.825	No
Cisco	2022-08-05	-0.000	0.819	0.050	0.434	No
Uber	2022-09-15	0.000	1.709	0.074	0.494	No
MGM Resorts	**2023-09-10**	**0.001**	**1.312**	**-0.141**	**0.032**	**Sí**
23andMe	2023-10-01	-0.005	2.027	-0.041	0.881	No
UnitedHealth	2024-02-21	0.000	0.220	-0.073	0.161	No
Live Nation	2024-05-27	-0.000	1.115	-0.103	0.255	No
JPMorgan Chase	2014-10-05	0.000	1.162	-0.005	0.902	No
eBay	2014-05-21	-0.001	1.065	-0.031	0.446	No
Under Armour	2018-03-29	-0.001	1.413	0.103	0.320	No
Community Health Systems	2014-08-18	-0.000	1.047	0.099	0.075	No
Total				-2.146		

Tabla C.4: Eventos y CAR para la ventana (-10,10)

APÉNDICE D

Anexo D: Muestra de las empresas de control seleccionadas

Empresa Afectada	Empresa de Control	Justificación del Emparejamiento
Target	Walmart	Competidor directo en el sector minorista (retail), con modelo de negocio y escala comparables.
T-Mobile	Verizon	Rival directo en el sector de las telecomunicaciones en Estados Unidos.
Equifax	TransUnion	Competidor directo, siendo dos de las tres principales agencias de crédito.
Toyota	General Motors	Fabricantes de automóviles consolidados y competidores globales directos.
Clorox	Kimberly-Clark	Competidores en el sector de bienes de consumo envasados y productos para el hogar.
Intel	AMD	Duopolio principal en el mercado de procesadores (CPU) para ordenadores y servidores.
Snowflake	Datadog	Empresas líderes y competidoras en el sector de plataformas de datos en la nube (Cloud Data).
CrowdStrike	Palo Alto Networks	Compañías líderes y competidoras directas en la industria de la ciberseguridad.
Sony	Samsung	Conglomerados de electrónica de consumo diversificados y competidores directos en múltiples segmentos.
Marriott	Hilton Worldwide	Dos de las mayores cadenas hoteleras del mundo y competidores directos en el sector de la hostelería.
Facebook	Alphabet (Google)	Gigantes tecnológicos cuyo principal modelo de negocio es la publicidad digital.
Capital One	American Express	Entidades financieras líderes en la emisión de tarjetas de crédito y servicios financieros.

Tabla D.1 – continuación de la página anterior

Empresa Afectada	Empresa de Control	Justificación del Emparejamiento
Microsoft	Alphabet (Google)	Gigantes tecnológicos que compiten directamente en servicios en la nube (Azure vs. GCP) y software.
T-Mobile	AT&T	Rival directo en el sector de las telecomunicaciones en Estados Unidos.
Nvidia	AMD	Duopolio principal en el mercado de unidades de procesamiento gráfico (GPU).
Cisco	Juniper Networks	Competidores históricos en el sector de hardware y equipos de redes (networking).
Uber	Lyft	Duopolio principal en el mercado de transporte compartido (ride-sharing) en Estados Unidos.
MGM Resorts	Caesars Entertainment	Operadores líderes y competidores directos en la industria de casinos y complejos turísticos.
23andMe	Ginkgo Bioworks	Empresas públicas competidoras en el sector de la biotecnología y la genómica.
UnitedHealth	Elevance Health	Dos de las mayores aseguradoras y proveedoras de servicios de salud en Estados Unidos.
Live Nation	Madison Square Garden	Empresas líderes en el sector del entretenimiento en vivo y la gestión de recintos.
JPMorgan Chase	Bank of America	Dos de los cuatro bancos más grandes de EE.UU., competidores en banca minorista y de inversión.
eBay	Best Buy	Competidores en el comercio minorista online y físico de bienes de consumo y electrónica.
Under Armour	Nike	Competidores directos y líderes en el mercado de ropa y calzado deportivo.
Community Health	Tenet Healthcare	Competidores en la operación de redes de hospitales y centros de atención médica en EE.UU.

Tabla D.1: *Composición de la Muestra, Grupo de Control y Justificación del Emparejamiento*

Facultad de Administración y Dirección de Empresas /UPV

DECLARACIÓN DE USO DE INTELIGENCIA ARTIFICIAL GENERATIVA (IAG) EN EL TFG–FADE / UPV

1. Indica el uso realizado de la Inteligencia Artificial Generativa (IAG):

☐ NO he utilizado herramientas de IAG en el desarrollo del TFG

☑ SÍ he utilizado herramientas de IAG en el desarrollo del TFG.

2. Si has utilizado herramientas de IAG, indica cuáles

Claude Code

3. **Declaración ética y legal.** Confirmo que al utilizar la IAG:

☑ No he facilitado datos confidenciales sin autorización.

☑ No he utilizado materiales protegidos por derechos de autor sin permiso o sin acogerse a una excepción legal (dominio público, licencias CC o derecho de cita).

☑ No he introducido datos personales sin autorización.

☑ He respetado los términos de uso de las herramientas y no las he empleado de forma engañosa, fraudulenta o maliciosa.

4. **Descripción del uso técnico**. Declaro haber hecho uso de herramientas de IAG (ChatGPT, Gemini, Copilot u otras) en los siguientes apartados del TFG y para las tareas que se detallan a continuación:

	Documentación / búsqueda de información	Revisión o reescritura de texto propio	Apoyo en análisis o tratamiento de datos	Generación esquemas o gráficos	Traducción o resumen bibliografía	Presentación
Introducción	SI	SI	NO	NO	NO	NO
Marco Teórico	SI	SI	NO	NO	NO	NO
Metodología	SI	NO	NO	NO	NO	NO
Resultados / análisis de datos	SI	NO	SI	NO	NO	NO
Discusión / propuestas mejora	SI	SI	SI	NO	NO	NO
Conclusiones	SI	SI	NO	NO	NO	NO
Referencias bibliográficas	SI	SI	NO	NO	NO	NO
Presentación o materiales complementarios	SI	NO	NO	NO	NO	NO

Este documento se ha elaborado en el marco del Proyecto de Innovación Docente PIME 25/26-569 financiado por la UPV.

5. Indica qué **tipo de IAG** has utilizado en los distintos apartados del TFG (si aplica):

	IAG Texto	IAG búsqueda y gestión bibliográfica	IAG código	IAG imágenes o multimedia	IAG análisis de datos o modelado
Introducción	SI	SI	NO	NO	NO
Marco Teórico	SI	SI	NO	NO	NO
Metodología	SI	SI	NO	NO	NO
Resultados / análisis de datos	NO	NO	SI	NO	NO
Discusión / propuestas mejora	SI	NO	NO	NO	NO
Conclusiones	NO	NO	NO	NO	NO
Referencias bibliográficas	NO	SI	NO	NO	NO
Presentación o materiales complementarios	NO	NO	NO	NO	NO

6. **Ejemplos**. Indica, al menos, tres ejemplos de instrucciones o prompts que has utilizado al interactuar con herramientas de IAG (si procede).

"Explicame cual es el modelo de Fama French de tres factores y dame referencias dónde pueda documentarme".

"Cómo reescribirías este párrafo de manera que enlace con los contenidos de la sección _"

"Que librerías puedo utilizar para el análisis de datos con python que voy a realizar en el proyecto"

En todas ellas habría mucho más contexto, lo cual le permite a la IA adecuarse a cada una de las tareas del proyecto de manera correcta

7. **Reflexión personal.** En una o dos frases, valora brevemente las fortalezas y limitaciones del uso de la IAG en tu trabajo y si te ha ayudado en tu proceso de aprendizaje.

Como futuro graduado en Administración y Dirección de Empresas, así como de Ingeniería Informática, considero que los Modelos Extensos de Lenguaje (LLM's) han llegado para quedarse. La IA es una tecnología muy potente, que tiene la capacidad de guiar al usuario de manera directa en la tarea que desea realizar. Si bien es cierto que hoy existen múltiples aplicaciones, la mejor sin duda es la facilidad con la que se puede obtener información relevante sobre un tema en concreto y encontrar referencias que permitan desarrollar el trabajo. Si bien es cierto, no todo es del color de rosa, los modelos pueden equivocarse (y lo harán múltiples veces), en un proceso que se llama "Alucinación", por lo que es de vital importancia que el propio estudiante

Firma del estudiante Alonso Veliz Garcia Fecha: 10-03-2026

Este documento se ha elaborado en el marco del Proyecto de Innovación Docente PIME 25/26-569 financiado por la UPV.