PANORAMA ECONÓMICO, vol. XVI, núm. 33, enero-junio, 2021, pp. 119-136

Impacto en el precio de las acciones de los bancos debido al ataque cibernético al SPEI

Sergio Rodolfo Góngora Jiménez[*] Humberto Banda-Ortiz[**]

(*Recibido: marzo,* 2020/*Aceptado: julio,* 2020)

Resumen

Durante 2018, un grupo de ciberataques exitosos a algunos bancos mexicanos, demostró el riesgo a lo que están expuestos. El objetivo del presente artículo es identificar el impacto económico en el precio de las acciones de los bancos debido al ataque cibernético al sistema de pagos interbancario mexicano (SPEI). La metodología utilizada uso diferentes indicadores financieros comúnmente usados para valorar el riesgo reflejan el impacto económico en el precio de las acciones de los bancos afectados. En los resultados se observa como los indicadores Beta, Alpha, Treynor, Sharpe y VaR relacionan las fechas de los ataques y el impacto en el precio de las acciones. Cuando se realiza un análisis con dichos indicadores utilizando una periodicidad diaria, su demuestra el impacto económico sufrido pese a que algunas instituciones bancarias no difundieron oportunamente la información a sus accionistas.

Palabras clave: cibercrimen; ciber-seguridad; bancos; sistema interbancario de pagos electrónicos; SPEI.
Clacificación JEL: O33, L86, G21.

[*] Doctorante en la Universidad Autonóma de Querétaro. <Sgongora65@hotmail.com>
[**] Profesor-investigador en la Universidad Autonóma de Querétaro. <humberto.banda@gmail.com>.

Impact on the price of bank shares due to the cyber-attack on the SPEI

Abstract

During 2018, a group of successful cyber-attacks on some banks demonstrated the risk to which they are exposed. The target of this article is to identify the economic impact on the price of bank shares due to the cyber-attack on the Mexican interbank payment system (SPEI). The importance in economic terms of the interbank electronic payment system has made it an objective for cybercriminals. The methodology used uses different financial indicators commonly used to assess risk reflect the economic impact on the price of the shares of the banks. The results show how the indicators Beta, Alpha, Treynor, Sharpe and VaR relate the dates of the attacks and the impact on the price of the shares. When an analysis is carried out with these indicators using a daily periodicity, it demonstrates the economic impact suffered despite the fact that some banking institutions didn't timely disseminate the information to their shareholders.

Keywords: cybercrimes; cybersecurity; private banks; the interbank electronic payment system.
JEL classification: O33, L86, G21.

1. Introducción

Los progresos que se han tenido durante las últimas décadas en las tecnologías de la comunicación y, específicamente, en la infraestructura de internet proporciona un ambiente propicio para la realización de actividades ilegales. Actualmente, el tráfico de Internet se expande considerablemente en todos los países, lo que contribuye significativamente a una mayor exposición por parte de los agentes económicos a los ataques de delitos informáticos. Más allá de las ventajas inherentes de la integración internacional, las TIC's (Tecnologías de Información y Comunicaciones) proporcionan un entorno propicio para obtener beneficios ilegales basados sobre actividades complejas relacionadas con delitos cibernéticos, especialmente en términos de países emergentes.

Un ejemplo de lo planteado en el párrafo anterior es que durante 2018 algunos bancos mexicanos sufrieron ataques exitosos por parte de hackers, a pesar de las medidas implementadas por las autoridades del sistema financiero mexicano para proteger a las instituciones de los ciberataques.

Dicho evento pone de manifiesto el riesgo al que están expuestas las instituciones financieras. Es por ello que la implementación de estrategias de seguridad y protección cibernética deben alcanzar un nivel superior, tanto en términos de tecnología como de recursos asignados. De acuerdo con la firma de consultoría Pricewaterhouse Coopers (2014), el 45% del sistema financiero a nivel mundial ha sufrido ataques informáticos, en comparación con las demás industrias, las cuales reportan que un 34% han sufrido ciberataques.

Por lo que respecta al impacto económico que tienen los ciberataques, diferentes estudios muestran que las empresas sufren una perdida, a corto plazo, de entre el 1% y el 5% en el precio de sus acciones. No obstante, en lo referente a las instituciones financieras dicha perdida puede llegar hasta el 15%. Es por ello que el objetivo del presente estudio es identificar el impacto económico en el precio de las acciones de los bancos debido al ataque cibernético al sistema de pagos interbancario mexicano (SPEI).

La presente investigación se estructura de la siguiente manera: en la segunda sección se presentan los diferentes estudios sobre los ataques cibernéticos y su impacto en la economía. En la tercera sección se presenta una breve descripción del sistema bancario mexicano y del sistema de pagos electrónicos interbancarios (SPEI). En la cuarta sección se presenta la metodología para analizar el impacto que tuvieron los bancos mexicanos por el ataque al SPEI. En la quinta sección se presentan los resultados de la investigación. Finalmente, en la sexta sección se presentan las conclusiones.

2. Estado del Arte

De acuerdo a Antonescum (2015), en términos generales, el delito cibernético se incluye como una actividad completamente ilegal y criminal que se lleva a cabo a través de tecnología de la información. Las afectaciones generadas por el delito cibernético son ampliamente discutidas en la literatura. Autores como Martínez (2018), han analizado el tema del delito cibernético proporcionando ideas fundamentales para minimizar el riesgo de ataques o, incluso, combatir este fenómeno negativo.

De acuerdo a Gómez (2017), en general, el delito cibernético incluye una amplia gama de actividades ilegales como: acoso cibernético, terrorismo cibernético, robo de identidad, acoso cibernético, pornografía virtual (a través de Internet), espionaje cibernético (obtención ilegal datos confidenciales), piratería informática, fraude informático, acoso en línea, phishing, piratería en línea, chantaje virtual, extorsión cibernética, ataques de spam, infracción de derechos de autor, virus informáticos instalados sin conocimiento del usuario de programas de software malicioso.

Saini, Rao y Panda (2012), examinaron el impacto de las amenazas cibernéticas a raíz de problemas como interrupción económica, trastorno psicológico, ataques a la seguridad nacional (defensa) para realizar fraudes y actividades ilegales. En este mismo sentido, otros autores como Espinosa (2015), identifican las siguientes categorías de ciberdelincuentes, junto con las especificaciones correspondientes de cada categoría: ciber terroristas, piratas cibernéticos, hackers, delincuentes profesionales, crackers y bromistas.

De acuerdo al estudio publicado por PricewaterhouseCoopers (2014), indica que el 45% del Sistema financiero mundial ha sufrido ataques informáticos en comparación con las demás industrias que reportan el 34%. Este sector sigue siendo un objetivo clave para los ciberdelincuentes y la apropiación indebida de activos económicos sigue siendo el principal tipo de delito denunciado.

Anderson & Moore (2014), denotan la importancia de los sistemas de información electrónica es evidente para todos los participantes en la economía moderna. Cuando la información no circula, sectores enteros de la economía es vulnerable. Los sectores financieros, el comercio mayorista y minorista, transporte público, la industria, y las empresas de servicios se ralentizarían debido a la falta o deterioro de sus sistemas informáticos. Los servicios públicos vitales son igualmente dependientes de la tecnología de la información y comunicaciones.

Para Machín & Gazapo (2016), la seguridad de la información, la protección de los sistemas informáticos, la integridad, confidencialidad y disponibilidad de los datos que contienen, se reconocen como un aspecto crítico de política nacional. Se han identificado dos tendencias actuales que indican su importancia es creciente: En primer lugar, la integración de las computadoras en más y más aspectos de la modernidad de la vida cotidiana. En segundo lugar, los ciberataques o las infracciones de seguridad en la información parecen aumentar en frecuencia, y pocos observadores están dispuestos a ignorar la posibilidad que futuros ataques podrían tener consecuencias mucho más severas de lo que ha sido observado hasta la fecha.

De acuerdo al estudio presentado por Cashell (2004), sobre el impacto económico de los ciberataques, indican que las empresas que anuncian una violación de seguridad informática sufren una perdida a corto plazo entre el 1% y el 5% del precio de sus acciones y en el caso de empresas financieras pueden llegar hasta el 15%, en donde los atacantes obtuvieron acceso a información confidencial de sus clientes.

Las investigaciones sobre el impacto en el precio de las acciones de los ciberataques muestran que identificó que las empresas objetivo de los ciberataques sufren pérdidas, las caídas de precios rondan las magnitudes de pérdidas de accionistas de entre $ 50 millones y $ 200 millones.

De acuerdo a la teoría de mercado, el precio de las acciones de una empresa está determinado principalmente por el valor presente descontado

de los flujos de efectivo que se espera que resulten de la producción de esa empresa. Ese flujo de caja es lo que contribuye a la riqueza de los accionistas, ya sea en forma de dividendos o en la expansión del *stock* de capital productivo de la empresa. Cualquier evento eso cambia las expectativas de los inversores sobre ese flujo futuro de ingresos que probablemente afectar el precio de la acción.

Brown, Edwards y Marsden (2009), investigaron los complejos problemas asociados a la seguridad de la información y el creciente grado de exposición, así como, la importancia que han adquirido para los gobiernos, las corporaciones y la sociedad actual.

Lagazio, Sherif y Cushman (2014), investigaron los efectos de los delitos informáticos en el sector financiero y revelaron ciertas vulnerabilidades con respecto al comportamiento estratégico de las compañías financieras, tales como, gastos exagerados de defensa y una persistente negación o desestimación de incidentes de delitos cibernéticos.

Según Cashell & William (2004), nadie en el campo está satisfecho con nuestra capacidad actual para medir los costos y probabilidades de ciberataques. No existen metodologías estándar para el análisis de costos y su medición, y el estudio de la frecuencia de los ataques se ve obstaculizado por la renuencia de organizaciones para hacer públicas sus experiencias con violaciones de seguridad. Existen diversos incentivos para no revelar información sobre un ciberataque. Lo que genera falta de información y datos sobre violaciones de seguridad de la información, no porque la información no se cuantifique, más bien, el problema es que las organizaciones tienen incentivos económicos reales para no revelar dicha información. Los costos de la divulgación al público pueden tomar varios efectos:

- Impacto en el mercado financiero. Los mercados de acciones, crédito y los bonos las emitidos por las empresas, así como su calificación pueden reaccionar negativamente a los anuncios de violación de seguridad.
- Reputación o efectos de confianza. La publicidad negativa puede dañar la reputación o marca de una empresa, e incluso, hacer que los clientes pierdan confianza. Estos efectos pueden dar a sus rivales comerciales una competencia ventaja.
- Problemas de litigio. Si una organización informa una violación de seguridad informática, los inversores, los clientes u otras partes interesadas pueden utilizar los tribunales para buscar la recuperación de daños.
- Problemas de responsabilidad. Los funcionarios de una empresa u organización pueden enfrentar sanciones bajo leyes federales como La Ley Federal de Protección de Datos Personales en Posesión de Particulares de México, en caso de tener información de clientes de EU. Ley de 1999 (GLBA) o la Ley Sarbanes-Oxley de 2003.

- Señal a los atacantes. Un anuncio público puede alertar a los piratas informáticos de que las ciber defensas de una organización son débiles e inspiran aún más ataques
- Seguridad en el empleo. El personal de TI (Tecnologías de la Información) puede temer por sus trabajos después de un incidente y tratar de ocultar la violación de seguridad a la alta dirección.

Cualquiera de estos costos de divulgación puede ser significativo. Pueden seguir rápidamente a un anuncio público y están a cargo de empresas individuales o individuos dentro de esas empresas. De acuerdo a Gómez (2017), las posibles víctimas a menudo descuidan la idea de la vulnerabilidad al delito cibernético y sus amplias implicaciones negativas. Los principales canales utilizados en los delitos cibernéticos incluyen componentes de uso común de internet, como, correos electrónicos, sitios web (en particular, sitios de comercio electrónico), salas de chat, grupos de discusión, mensajería instantánea (IM), foros abiertos, redes sociales, mensajería u otros servicios en línea. Las implicaciones financieras de los delitos cibernéticos representan un tema muy delicado en el contexto de economías globalizadas.

Según Antonescum (2015), indica que los países emergentes representan un objetivo muy vulnerable debido a problemas estructurales y desequilibrios institucionales. Desde el uso creciente de la tecnología de la información, las posibilidades de obtener ganancias fraudulentas con base en delitos cibernéticos se han vuelto cada vez más significativas. Debido a los ciberataques, el rendimiento de la empresa se ve afectado significativamente y también aumentan las pérdidas financieras. Aparentemente, el efecto acumulativo de los delitos cibernéticos proporciona un marco inquietante sobre la fragilidad de las economías emergentes con respecto a cualquier tipo de ciberataques, como manipulación del mercado y obtención de códigos de acceso a las cuentas bancarias de los clientes. Sin embargo, hay es una ventaja importante relacionada con el bajo nivel de desarrollo de las economías emergentes en comparación con países desarrollados. Por lo tanto, el uso de la tecnología de la información y, en consecuencia, Internet no es muy elevado y extenso para los países emergentes, pero existe una fuerte tendencia de crecimiento al alza.

De acuerdo con lo planteado por Generali Global Assistance (2018), las implicaciones no financieras de los delitos cibernéticos incluyen una serie de cuestiones extremadamente importantes como: pérdida de confianza del cliente, publicidad negativa (escándalos de imagen, daño a la reputación), disminución de la productividad, discontinuidad del servicio de negocio, pérdida de datos o información confidenciales de clientes o empresas, acceso no autorizado a ciertas innovaciones de productos, pérdida de propiedad intelectual, etc., a veces es muy difícil estimar con precisión el costo del delito cibernético ataca considerando ciertas implicaciones no financieras. Además,

las implicaciones no financieras de los delitos cibernéticos son bastante difíciles de comparar en función de un enfoque cuantitativo, pero sin duda tiene un Impacto muy alto con consecuencias extremadamente dramáticas.

3. Sistema bancario mexicano

En términos generales el SBM (Sistema Bancario Mexicano) representa uno de los dos sub - segmentos financieros en una economía; el otro está constituido por la Bolsas Mexicana de Valores y los intermediarios bursátiles "Casas de Bolsa" que operen en la economía. En el SBM actúan como intermediarios realizando operaciones de crédito mediante la recepción y el otorgamiento de créditos directos de y hacia los clientes. Esto es, por una parte, el banco capta recursos directamente de los ahorradores para posteriormente colocarlos como créditos directos a los prestatarios que solicitan los recursos.

De acuerdo a la página oficial del Banco de México (2019), La principal función de un sistema bancario es intermediar entre quienes tienen y quienes necesitan dinero. Quienes tienen dinero y no lo requieren en el corto plazo para pagar deudas o efectuar consumos desean obtener un premio a cambio de sacrificar el beneficio inmediato que obtendrían disponiendo de esos recursos. Dicho premio es la tasa de interés. Quienes requieren en el corto plazo más dinero del que poseen, ya sea para generar un valor agregado mediante un proyecto productivo (crear riqueza adicional) o para cubrir una obligación de pago, están dispuestos a pagar, en un determinado periodo y mediante un plan de pagos previamente pactado, un costo adicional por obtener de inmediato el dinero. Ese costo es la tasa de interés. Empatar las necesidades y deseos de unos, los ahorradores, con las necesidades de otros, los deudores, es la principal tarea del sistema financiero y en dicha labor las tasas de interés juegan un papel central.

El Banco de México tiene entre sus finalidades la promoción del sano desarrollo del sistema financiero a fin de lograr un sistema estable, accesible, competitivo y eficiente. Un sistema financiero con estas características facilita el cumplimiento de las tareas del banco central. A través del sistema bancario, un banco central pone en circulación la moneda nacional e instrumenta las políticas monetaria y cambiaria. La instrumentación de dichas políticas, a su vez, afecta los precios que se determinan en los mercados financieros, tales como las tasas de interés o el tipo de cambio.

3.1. El sistema de pagos electrónicos interbancarios (SPEI)

De acuerdo al sitio oficial de Banco de México (2019), el SPEI es un sistema de transferencias electrónicas de fondos que pertenece a y es operado por el

Banco de México. Este sistema se desarrolló con el objetivo de facilitar los pagos entre las instituciones financieras, además de habilitarlas para ofrecer a la población servicios de pago al menudeo de forma segura y eficiente.

El SPEI permite a sus participantes realizar pagos en pesos mexicanos por cuenta propia y a nombre de sus cuentahabientes, prácticamente en tiempo real, las 24 horas del día, todos los días del año. El funcionamiento del SPEI se sustenta en un marco jurídico basado en la Ley de Sistemas de Pagos, de la cual se deriva que la compensación y liquidación de las órdenes de transferencia aceptadas por este sistema son firmes, irrevocables, exigibles y oponibles frente a terceros, con lo que se asegura la finalidad de las operaciones.

El gobierno corporativo del SPEI está alineado al marco normativo y a las políticas del Banco de México. En este marco y políticas están contenidos los objetivos y funciones de la institución, su estructura orgánica, las atribuciones del Gobernador y de la Junta de Gobierno del Banco de México, así como de las unidades administrativas que dependen de estos y los mecanismos de rendición de cuentas, entre otros aspectos que son relevantes para el funcionamiento del SPEI.

De acuerdo a la página oficial del Banco de México (2018), el SPEI liquida en promedio alrededor de 400 mil pagos al día con un monto de más de 600 mil millones de pesos. Por otra parte, el fallo de un sistema de pagos que, aunque procese pagos de importe bajo tenga un número de operaciones muy alto, puede desencadenar una crisis generalizada en la economía. Por ejemplo, si a fin de mes dejara de funcionar el sistema de pagos al menudeo, muchos trabajadores dejarían de recibir sus salarios. Esta situación podría causar un malestar generalizado que afectaría a todo el país. Los ciudadanos perderían la confianza en el sistema bancario y posiblemente muchos de ellos preferirían cobrar su salario en efectivo.

Las personas físicas y morales pueden transferir recursos a través del SPEI por medio de instrucciones al banco que maneja su cuenta. Los bancos que ofrecen este servicio reciben instrucciones de sus clientes para estas operaciones desde diversos canales, tales como portales de Internet, aplicaciones de banca móvil, mensajes vía SMS y ventanillas de sus sucursales.

3.2. Las instituciones que participan en el SPEI

Son las instituciones financieras reguladas, las cámaras de compensación autorizadas por el Banco de México en términos de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros y otras entidades reguladas y supervisadas por el Banco de México, la Comisión Nacional Bancaria y de Valores (CNBV), la Comisión Nacional del Sistema de Ahorro para el Retiro (CONSAR) y la Comisión Nacional de Seguros y Fianzas (CNSF),

que el propio Banco de México autorice. A finales de diciembre de 2015, los participantes en el SPEI incluían a 52 instituciones financieras bancarias y 55 instituciones financieras no bancarias, las cuales utilizan el sistema para realizar los pagos relacionados con su propia operación, además de que algunas de ellas, como los bancos y las sociedades financieras populares, también lo utilizan para ofrecer servicios de pago a sus clientes.

4. Metodología

Para analizar, el impacto que tuvo el ataque al SPEI en los bancos mexicanos, y siguiendo lo planteado por Vázquez (2010), se debe considerar que el precio de las acciones está ligado a los resultados de las empresas, es decir, está relacionado a las expectativas sobre el futuro de las ganancias o pérdidas, por lo tanto, al sufrir un ciberataque donde se afectan las utilidades de la empresa, se genera un impacto que se ve reflejado en mayor o menor medida en el valor de las acciones, considerando que los hechos ocurrieron durante 2018, el estudio relaciona las fechas de los ciberataques con los cambios en precios de sus acciones derivados del riesgo operativo que sufrieron los bancos.

Los datos de los precios de las acciones de los bancos que cotizan en el mercado bursátil en México tienen como origen principal la Bolsa Mexicana de Valores, que fue la información diaria para periodo de estudio. De la misma manera, se obtuvo el índice la BMV denominado IPC (Índice de Precios y Cotizaciones), también de manera diaria, con la finalidad de tener homologada toda la información requerida de la presente investigación.

Con los datos históricos diarios de 2018 de los bancos afectados, además del IPC de la BMV, se integraron en una sola tabla denominada matriz de precios. Con dicha información se genera la matriz de rentabilidades que es la fuente principal de información para nuestro estudio, a partir de ella, se calcularon todos los indicadores utilizados.

A continuación, se describen todos los indicadores que se utilizaron en el presente estudio, iniciando por la matriz de rentabilidades, para la cual se utiliza la siguiente formula (1), para cada uno de los bancos, de igual manera para índice IPC.

$$RDA = Ln\frac{PAD^1}{PAD^2} \tag{1}$$

En donde:

RDA = Rentabilidad diaria de la acción
LN = Logaritmo natural

*PAD*1 = Precio de la acción del día
*PAD*2 = Precio de la acción del día de ayer

El indicador Beta es una medida de la volatilidad de la acción a estudiar con referencia al índice, este estudio utilizo como referencia IPC (Índice de Precios y Cotizaciones). En el caso del indicador Alpha se define como el exceso de rendimiento de una inversión en relación con el rendimiento de un índice de referencia, es decir el IPC.

Para el análisis, se utilizarán las fórmulas para el cálculo de Beta (2) y Alpha (3), con la finalidad de obtener el mayor detalle posible en todos nuestros cálculos usamos rentabilidades diarias.

$$\text{Beta} = \frac{(PAD - PA2018) * (PID - PI2018)}{(PID - PI2018)} \qquad (2)$$

En donde:

PAD = Precio de la acción del día de cada banco
*PA*2018 = Promedio de la acción durante 2018
PID = Precio del IPC del día
*PI*2018 = Promedio del IPC durante 2018

La fórmula para el cálculo del indicador Alpha.

$$\text{Alpha} = \text{RAD} - \text{TLMD} - \text{BAD} * (\text{RID} - \text{TLMD}) \qquad (3)$$

En donde:

RAD = Rentabilidad de la acción diaria
TLMD = Tasa libre de mercado con base en TIIE 28 días diaria publicada por Banco de México.
BAD = Beta de la acción diaria
RID = Rentabilidad del IPC diario

Estas dos medidas son utilizadas en los análisis de sensibilidad, que permiten correlacionar las fechas de los ataques al SPEI y la cotización de las acciones de los bancos afectados.

Para profundizar más la investigación y analizar más a detalle se integraron los indicadores de Sharpe, Treynor y VaR (Value at Risk), el indicador de Sharpe nos ayudar a comprender el retorno de una inversión en comparación con el riesgo.

La fórmula para el cálculo del ratio Sharpe:

$$\text{Sharpe} = \frac{\frac{(Promedio\ \ (RAD^1 : RAD^2) - Promedio\ \ (TLM^1 - TLM^2)}{100}}{DesvEst.p(RAD^1 : RAD^2)} \qquad (4)$$

En donde:

RAD[1] = Rentabilidad de la acción del día
RAD[2] = Rentabilidad de la acción del día de ayer
TLM[1] = Tasa libre de mercado del día con base en TIIE 28 días diaria publicada por Banco de México.
TLM[2] = Tasa libre de mercado del día de ayer con base en TIIE 28 días diaria publicada por Banco de México.
DESVEST.P = Desviación estándar en función de la población total

El ratio de Treynor también busca evaluar el rendimiento ajustado por riesgo, pero mide el rendimiento en comparación con un punto de referencia diferente. En lugar de medir el rendimiento con la tasa de rendimiento libre de riesgo, la relación de Treynor busca examinar qué tan bien una cartera supera al mercado de valores en su conjunto, lo que permite analizar incremento en el riesgo observado en el precio de las acciones.

La fórmula para el cálculo del indicador Treynor:

$$\text{Treynor} = \frac{\frac{(Promedio\ \ (RAD^{1}:RAD^{2}) - Promedio\ \ (TLM^{1} - TLM^{2})}{100}}{BAD} \tag{5}$$

En donde:

RAD[1] = Rentabilidad de la acción del día
RAD[2] = Rentabilidad de la acción del día de ayer
TLM[1] = Tasa libre de mercado del día con base en TIIE 28 días diaria publicada por Banco de México.
TLM[2] = Tasa libre de mercado del día de ayer con base en TIIE 28 días diaria publicada por Banco de México.
BAD = Beta de la acción diaria

Por último, el valor en riesgo "VaR" es una medida del riesgo de pérdida para las inversiones. Estima cuánto puede perder un conjunto de inversiones (con una probabilidad dada), dadas las condiciones normales del mercado, en un período de tiempo establecido, en nuestro caso se considera al igual que en los otros indicadores el riesgo día a día.

La fórmula para el cálculo el VaR al 95% es la siguiente:

$$\text{VaR} = F * S * \sigma * \sqrt{t} \tag{6}$$

En donde:

F = DISTR.NORM.ESTAND.INV (95%)
S = Desviación estándar (RAD^1 : RAD^2)
σ^2 = Varianza (RAD^1: RAD^2)
$\sqrt{t}$ = Raíz (1/252)

A continuación, se presentan los resultados obtenidos al aplicar la metodología presentada en esta sección.

5. Resultados

De acuerdo al modelo de valoración de activos CAPM (Capital Asset Princing Model) desarrollado por Jack L. Treynor, William Sharpe (1964), John Lintner (1965) y Jan Mossin (1966). Quienes desarrollan su modelo y teorías sobre el riesgo de mercado (también denominado sistemático) y como impactan en los rendimientos de las acciones de las empresas. Podemos analizar, como el precio de las acciones se pueden ver afectadas por las expectativas sobre las expectativas de utilidades de las empresas. Con este criterio, utilizaremos los coeficientes definidos en la sección anterior para relacionar como el precio de las acciones con las fechas de los ataques cibernéticos del SPEI.

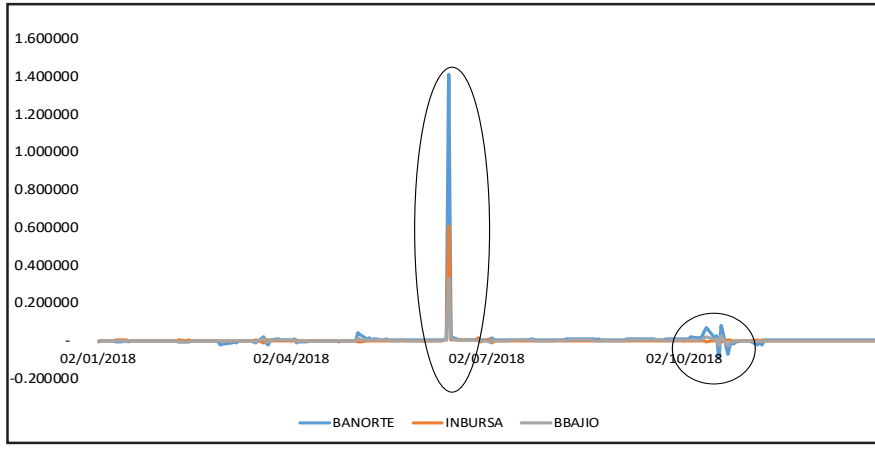
La matriz de rentabilidades es la fuente principal de información para nuestro estudio, a partir de ella, calculamos el coeficiente Beta (formula 1), dicho coeficiente establece una relación lineal entre la rentabilidad en exceso de los bancos sujetos a estudio y la rentabilidad del mercado en nuestro caso el IPC, como se comentó anteriormente, el coeficiente Beta representa la pendiente de la recta que relaciona el precio de la acción con el índice de referencia. Sin embargo, para definir completamente dicha recta es necesario agregar la constante por lo que a través de la fórmula 2 se define el Alpha de Jensen.

Estos indicadores, nos ayudan a establecer un análisis de sensibilidad de riesgo de mercado que sufrieron los bancos afectados durante los ataques informáticos al SPEI, tratando de correlacionar el comportamiento de los precios de las acciones y las fechas de los ciberataques.

En la figura 1, que se muestra a continuación se puede observar el indicador Beta aplicada a partir de la formula 1 presentada en la sección anterior.

Como se puede observar en la figura 1, los circulos representan las variaciones del coeficiente Beta con relación a las fechas de los ciberataques que sufrieron los bancos, dicho indicador muestra una variación en la rentabilidad de las acciones de los bancos, causada por el incremento en el riesgo de mercado que los inversionistas identifican derivado del ciberataque al SPEI, También se puede observar que en el segundo ataque, la sensibilidad de los inversionistas es menor, debido a que se pudo confirmar que dicho ataque no fue directamente dirigido a los bancos, sino más bien a otros intermediarios financieros como aseguradoras entre otros, sin embargo, el componente de nerviosismo entre los accionistas se vio reflejado como se ve reflejado en la figura 1.

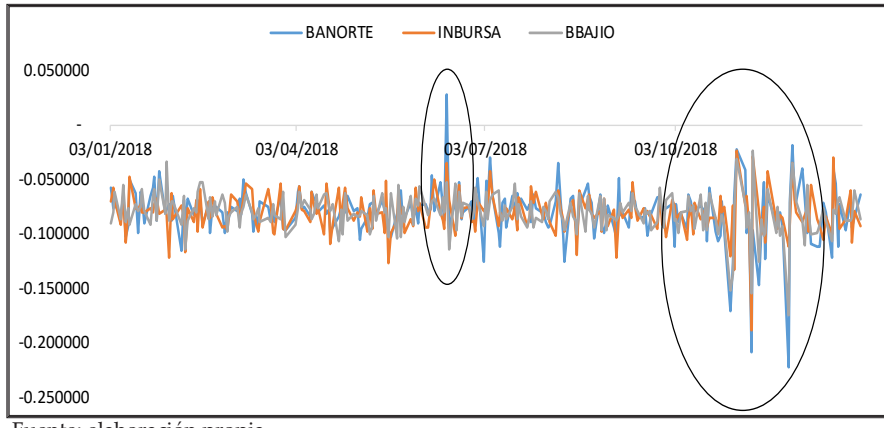
En el caso de Alpha de Jensen mide la rentabilidad extraordinaria de los bancos sobre su rentabilidad ajustada por el riesgo.



Fuente: elaboración propia

Figura 1
Indicador Beta

En la figura 2, se muestra el indicador Alpha de jensen, si bien en el primer ataque muestra una diferencia significativa, en las fechas del segundo ataque se muestra un incremento en el riesgo derivado a la sencibilidad de los inversionistas al riesgo mercado de los bancos afectados. En días siguientes a los ataques se ve como el indice de Jensen nos muestra como el rendimiento promedio de las acciones de los bancos es menor al rendimiento esperado de las acciones. Como se puede ver en las graficas anteriores, se debe considerar que existe el periodo de tiempo entre que un ataque informatico es detectado y la información se hace publica, se entiende que el periodo de volatilidad en el precio de las acciones en el tiempo se encuentra con un retraso, esto esta de acuerdo a lo publicado por PWC (2014).

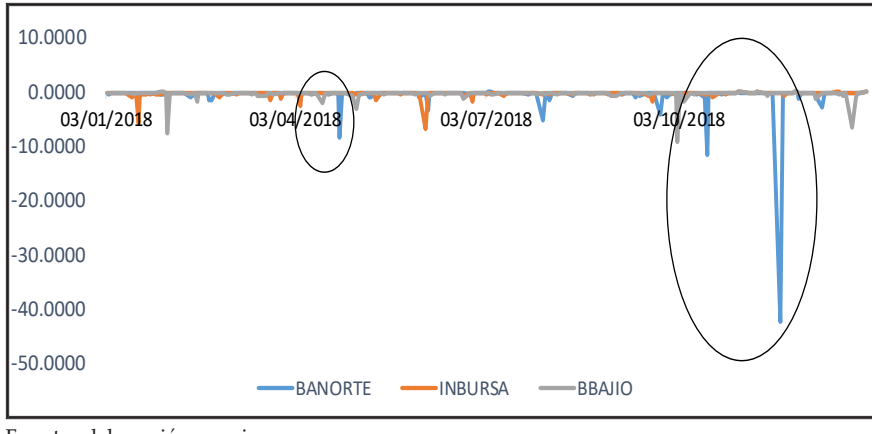


Fuente: elaboración propia.

Figura 2
Indicador Alpha de Jensen

Para profundizar la investigación y analizar más a detalle se calcularon los indicadores de Sharpe, Treynor y VaR (Value at Risk), el indicador de Sharpe nos ayudar a medir su riesgo en este caso de las acciones de los bancos contra los activos sin riesgo, Como se puede ver en la figura 3.

Según Gomero (2014) el índice de Sharpe contrasta el rendimiento promedio esperado contra los activos sin riesgo, además de la volatilidad de la cartera, para la presente investigación se seleccionó la TIIE 28 días, considerando que es la tasa de referencia del gobierno federal.



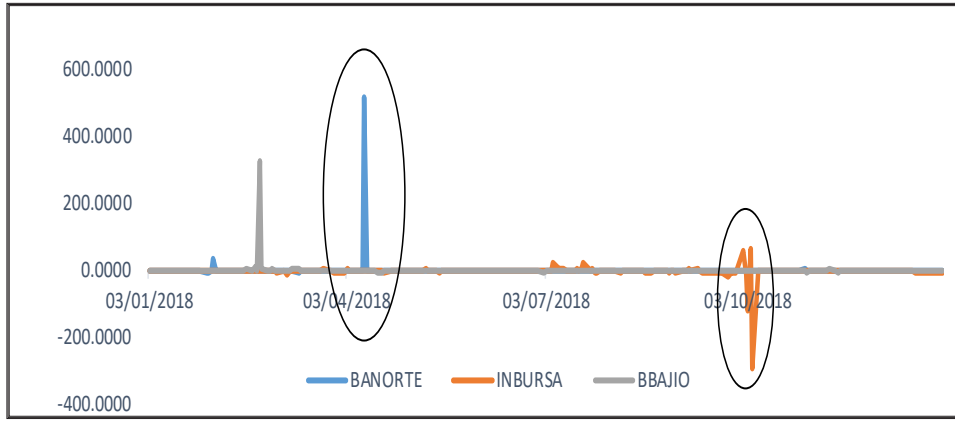
Fuente: elaboración propia

Figura 3
Indicador de Sharpe

De acuerdo con Gomero (2014), podemos ver que en las fechas cercanas a los ciberataques, el riesgo negativo indica un rendimiento de las acciones inferior en la rentabilidad al de un activo sin riesgo. De esta manera podemos identificar que en las fechas de los ataques y posteriormente la rentabilidad de las acciones de los bancos fue afectada, en referencia con la tasa libre de riesgo.

El indicador de Treynor busca evaluar el rendimiento ajustado por riesgo, pero mide la cartera en comparación con un punto de referencia diferente. En lugar de medir el rendimiento con la tasa de rendimiento libre de riesgo, la relación de Treynor busca examinar contra el mercado de valores en su conjunto. Esto se puede ver en la figura 4.

El ratio de Treynor mide el diferencial de la rentabilidad de la acción sobre el activo libre de riesgo, que es representada por el Beta. Lo que indica que a mayor ratio de Treynor mejor es la rentabilidad de las acciones, como podeos ver en la figura 4, el comportamiento de las acciones es muy plano, salvo los algunos días cercanos a los ciberataques al SPEI, que posiblemente se deba al incremento en el riesgo de mercado, lo que puede generar oportunidades de compra de las acciones.

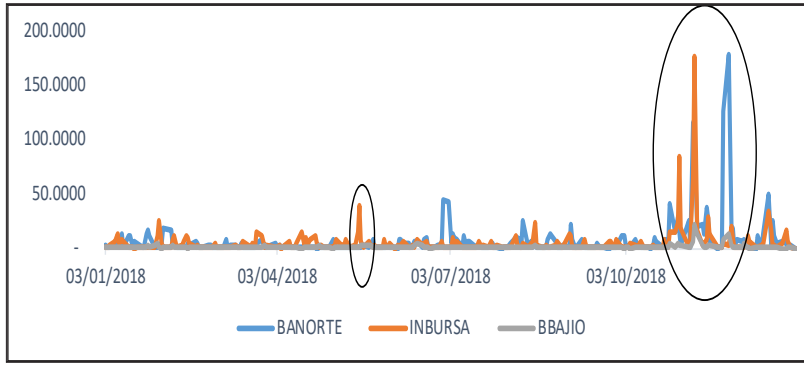


Fuente: eaboración propia.

Figura 4
Indicador de Treynor

De acuerdo a Montoya (2006), identifica al VaR (Value At Risk) como el método más generalizado de medir y estimar el riesgo de mercado de manera completa, en que se ve expuesto el rendimiento de una acción y se denomina como el máximo valor de perdida con un nivel de confianza especifico durante un periodo de tiempo determinado.

En nuestro estudio, el valor en riesgo (VaR) mide el riesgo de pérdida para las acciones de los bancos afectados por el ciber ataque al SPEI. Para su cálculo se considera al igual que en los otros indicadores el riesgo día a día con un valor de confianza del 5%. El comportamiento de este indicador de riesgo se puede observar en la figura 5.



Fuente: elaboración propia

Figura 5
Indicator VaR (Value At Risk)

Como se puede observar, en las fechas siguientes al segundo ataque se muestra una reacción en la rentabilidad de las acciones mayor al comportamiento normal, considerando el nivel de riesgo que los inversionistas perciben como un incremento en el riesgo de las acciones de los bancos afectados por el ciberataque al SPEI.

5. Conclusiones

El impacto económico de los ataques al SPEI, representaron un riesgo en la seguridad nacional, debido a que una falla en la seguridad informática en la infraestructura de los sistemas de pago representa un ataque al sistema financiero nacional en su totalidad. Los bancos afectados, como se puede ver en los resultados presentados, muestran un impacto económico que se ve reflejado en la cotización de sus acciones, lo que representa el aumento de riesgo que los inversionistas ven en los activos de los bancos.

Se demuestra que existió un retraso entre la detección del ataque sufrido y la divulgación del incidente, lo que demuestra un manejo opaco en la información pública de las empresas que cotizan en la bolsa, sin embargo, el efecto económico en el precio de las acciones se presentó, lo que confirmo que los indicadores de riesgo estudiadas de manera diaria sirven para identificar el impacto de los ciberataques en la economía de las empresas afectadas.

El efecto de los ciber ataques al SPEI, muestran que el primer ataque represento un impacto mayor que el segundo ataque, lo que representa que el segundo ataque fue más limitado que el primero, debido a que ya existía un procedimiento alterno probado de operación a través de un sistema de respaldo, lo que minimizo el impacto en los bancos analizados.

Referencias

Anderson R. y T. Moore (2014). *The economics of information security*. Article in Science november 2006. DOI: 10.1126/science.1130992. All content following this page was uploaded by Tyler Moore on 24 december 2014.

Antonescu, M. y R. Birau (2015). Financial and non-financial implications of cybercrimes in emerging countries. *Procedia Economics and Finance* 32 (2015), pp. 618-621.

Arias, L. y S. Rave (2006). Metodologías para la medición del riesgo financiero en inversiones. *Scientia et Technica Año XII*, núm. 32, diciembre 2006. UTP. ISSN 0122-1701.

Bouveret, A. (2018). Cyber risk for the financial sector: a framework for quantitative assessment. international monetary fund WP/18/143. *IMF working paper*. Disponible en: https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924

Brown, Ian and Edwards; Lilian and Marsden; T. Christopher (2009). Information security and cybercrime. Law and the internet, 3rd ed., L. Edwards, C. Waelde, eds., Oxford: Hart, 2009. Available at SSRN: https://ssrn.com/abstract=1427776.

Cashell, B., William J., *et al*. (2004). T*he Economic Impact of Cyber-Attacks*. CRS Report for USA Congress. Congressional Research Service, The Library of Congress. https://archive.nyu.edu/bitstream/2451/14999/2/Infosec_ISR_Congress.pdf.

Espinosa, E. (2015). Hacia una estrategia nacional de ciberseguridad en México. *Revista de Administración Pública, Instituto Nacional de Administración Pública (INAP)*, México, 136, enero-abril. https://www.academia.edu/12107238/Towards_a_Cybersecurity_Strategy_in_Mexico.

Generali Global Assistance (2018). The impact of cybersecurity incidents on financial institutions. https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf.

Gomero, N. A. (2014). Portafolios de activos financieros utilizando el modelo de Sharpe y Treynor. *Revista de la Facultad de Ciencias Contables*, vol. 22 núm. 41 pp. 135-146 (2014) UNMSM, Lima-Perú ISSN: 1560-9103 (versión impresa) / ISSN: 1609-8196 (versión electrónica).

Gómez, A. (2017). Enciclopedia de seguridad informática, 2da, ed. Editorial Ra-Ma.

Intsights (2019). Banking & financial services cyber threat landscape report april, 2019, https://intsights.com/resources/banking-financial-services-cyber-threat-landscape-report-april-2019.

Lagazio, M.; N. Sherif y M. Cushman (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. computers & security 4 5, 2014, pp. 58-74. www.sciencedirect.com.

Machín, N. y M. Gazapo (2016). La ciberseguridad como factor crítico en la seguridad de la unión europea, *Revista UNISCI*, núm. 42, octubre, 2016, pp. 47-68.

Martínez, C. (2018). Tendencias tecnológicas y desafíos de la seguridad informática. Polo de Conocimiento, ed. 19, vol. 3, núm. 5, mayo, 2018, pp. 260-279.

Pricewaterhouse Coopers (2014). Threats to the financial services sector. f*inancial services sector analysis of PwC's 2014 Global Economic Crime Survey*. https://www.pwc.com/gx/en/financial-services/publications/assets/pwc-gecs-2014-threats-to-the-financial-services-sector.pdf.

Randazzo, M.; M. Keeney y E. Kowalski (2005). Insider threat Study: Illicit cyber activity in the banking and finance sector. Technical report CMU/SEI-2004-TR-021, ESC-TR-2004-021. This work is sponsored by the US. Department of Defense. *The Software Engineering Institute is a federally funded research and development center sponsored by the US*. Department of Defense. Copyright 2005, Carnegie Mellon University.

Saini, H.; Y. Shankar y T. Panda (2012). *International Journal of Engineering Research and Applications* (IJERA) ISSN: 2248-9622 www.ijera.com, vol. 2, Issue 2, mar-april, 2012, pp. 202-209. Page Cyber-Crimes and their Impacts: A Review

Támara A.; I. Chica y A. Montiel (2017). Metodología de cálculo del Beta: Beta de los activos, Beta apalancado y Beta corregido por cash. *Revista Espacios*, vol. 38, núm. 34, año 2017, p. 15, ISSN 0798 1015.