Recuadro 1: Ciberataques en el sistema de pagos de alto valor CUD y su impacto sistémico

1. Introducción

El sistema de pagos de alto valor CUD es un componente esencial de la infraestructura de pagos del país. Esto se debe a que allí se da cumplimiento al extremo de dinero de las obligaciones contraídas en los mercados financieros (*i. e.*: mercado cambiario, renta fija, renta variable, derivados), así como el intercambio de fondos entre las entidades financieras después de la compensación neta multilateral de los instrumentos de pago electrónicos.

Los pagos entre las entidades participantes del CUD presentan alta interconectividad debido a que el pago realizado por una entidad es la fuente de liquidez de otra. De esta manera, la incapacidad de una entidad para realizar sus pagos puede, a su turno, afectar a otras, lo que desencadenaría eventos de carácter sistémico. Más aún, si se tiene en cuenta que los pagos realizados en un sistema como el CUD son de naturaleza crítica y urgente.

La dependencia creciente del sistema financiero, y en particular de las infraestructuras de mercado financiero, de tecnologías de información y comunicaciones para su operación y el procesamiento de la cuantiosa información que manejan, incrementa su exposición al riesgo cibernético. Esta vulnerabilidad se intensifica al depender de un conjunto de proveedores críticos de servicios esenciales (*hardware*, *software*, energía eléctrica y comunicaciones) para el funcionamiento continuo del sistema.

Según el documento *Cyber Resilience for Financial Market Infrastructures* publicado por Comité de Sistemas de Pago y Liquidación (CPMI, por su sigla en inglés) y el Comité Técnico de la Organización Internacional de Comisiones de Valores (Iosco, por su sigla en inglés) (CPMI-Iosco, 2012), el riesgo cibernético se define como: la combinación de la probabilidad de que ocurra un evento dentro del ámbito de los activos de información, los recursos informáticos y de comunicación de una organización y las consecuencias de ese evento para una organización.

Según Aldasoro *et al*. (2022), los eventos o métodos más comunes con que se realizan ciberataques son el *ransomware*, el robo de datos, *malware*, las secuencias de comandos entre sitios, la suplantación de identidad (*phishing*), el descifrado de contraseñas y los ataques de denegación de servicio. En este sentido, una alternativa para aproximarse al riesgo de ciberataques es a través del análisis de las consecuencias o impacto que sobre la dinámica de pagos en el CUD se presentaría si sus participantes fueran víctimas de un ataque cibernético.

Mediante el uso de simulaciones, se aborda el tema de lo que podría pasar con los pagos intradía que realizan las entidades si estas fueran objeto de un ataque cibernético. Para ello, y con base en lo señalado por Eisenbach, Kovner y Lee (2022a; 2022b), se toma en consideración una tipología de ataque individual y otra masiva. En la primera se seleccionan entidades con el mayor potencial de impacto sistémico en el CUD, de acuerdo con indicadores de importancia sistémica elaborados por el DSIF para el seguimiento a las infraestructuras financieras[1]. En el segundo, se tiene como criterio la indisponibilidad resultante de un ataque cibernético sobre el principal proveedor de servicios de comunicación que utilizan las entidades para conectarse al CUD. En ambos casos, se supone que el CUD se mantiene en funcionamiento.

Este recuadro presenta los incumplimientos de pagos resultantes (valor y número de entidades afectadas) de los escenarios descritos y también plantea una serie de medidas que podrían ser tenidas en cuenta para mitigar los riesgos asociados con un ataque cibernético. De esta manera, se brinda una perspectiva técnica que aborda el riesgo de ciberseguridad y, adicionalmente, se comparten elementos que pueden contribuir a la estabilidad y resiliencia del sistema financiero.

1 Teniendo en cuenta el número de contrapartes, cantidad y monto de operaciones, así como el papel que como distribuidor o receptor de pagos pueda tener.

Este recuadro se organiza en cinco secciones, incluida esta introducción. En la segunda se explican los principales elementos tenidos en cuenta para la construcción de los escenarios de simulación. En la tercera se analizan los resultados, haciendo énfasis en la manera como las entidades que no son afectadas por el evento de ciberseguridad podrían reaccionar. En la cuarta se incluyen consideraciones de política asociados con fortalecer la ciberseguridad. La quinta sección presenta las conclusiones y recomendaciones.

2. Consideraciones sobre el diseño de un escenario de ciberataque

El diseño de los escenarios que aquí se elaboran se soporta en la taxonomía de escenarios hipotéticos de ciberriesgo que Kaffenberger y Koop (2019) construyó sobre la propuesta de Atlantic Council (2016). Según este esquema los escenarios se pueden clasificar en tres grandes grupos: 1) riesgo operacional de alto impacto, 2) fallas de infraestructura ascendente y 3) choques externos y otros escenarios.

El listado de escenarios hipotéticos relacionados con el riesgo operacional lo componen: 1) bloqueo de *malware* o *ransomware* en una institución financiera; 2) transferencia bancaria fraudulenta; 3) violación de datos y fuga de información dirigida; 4) *malware* en sistemas de negociación; 5) ciberataque a gran escala en una red de mensajería global de transacciones financieras; y 6) ataque simultáneo sobre instituciones sistémicamente importantes. El grupo de escenarios vinculados a fallas de infraestructura ascendente incluye: 1) ataque de interrupción de la Cámara de Compensación Central; 2) ataque de interrupción de plataformas de procesamiento de pagos; 3) infección masiva por *malware*; 4) fallas de proveedor de servicios de nube; y 5) interrupción de servicios públicos con efectos dominó. Por su parte en el grupo de choques externos están los escenarios de: 1) ciberataque en retaliación a sanciones, y 2) conflicto armado.

Los escenarios hipotéticos que aquí se implementan para evaluar el impacto que sobre la liquidación de operaciones en el CUD tendría un ataque cibernético, se enmarcan en los grupos de riesgo operacional de alto impacto y de fallas de infraestructura ascendente de la propuesta de Kaffenberger y Koop (2019) y corresponden al Cuadro R1.1.

Cuadro R1.1
Escenarios simulados de ciberataque al CUD

Ciberataque simultáneo a entidades sistémicamente importantes	Ciberataque dirigido a proveedores de comunicaciones
Este podría ocurrir por el bloqueo que ocasionaría la inutilización de la mayoría de los computadores de un participante en el SPAV tras ciberataques por *malware* o *ransomware*. Este tipo de ataques ocurrieron con los virus Shamoon y el *ransomware* de WannaCry por la gran afectación que causó en el *hardware* y en el funcionamiento de un gran número de computadores.	Este podría ocurrir por el bloqueo que ocasionaría la ausencia del canal de comunicación entre las entidades y el CUD, como consecuencia de un ciberataque por *malware* o *ransomware* realizado al principal proveedor de telecomunicaciones. Lo anterior, reconociendo que la dependencia del sector financiero, incluidas las infraestructuras del mercado financiero, de los servicios de electricidad y las telecomunicaciones, los expone a riesgos que pueden impactar el funcionamiento de los mercados financieros y la actividad económica.
Dentro de la taxonomía de escenarios de riesgo cibernético de Kaffenberger y Kopp (2019), este tipo de ataque hace parte del grupo de riesgo operacional de alto impacto y corresponde de forma particular a los escenarios hipotéticos 1: de bloqueo operativo a una entidad financiera mediante un ataque de *malware* o *ransomware*, y 6: de ciberataque simultáneo a entidades sistémicamente importantes. Este tipo de ciberataque simulado es similar al realizado por Eisenbach, Kovner y Lee (2022a; 2022b) a los cinco principales bancos participantes en Fedwire.	Kaffenberger y Koop (2019) clasifican este escenario dentro del grupo de fallas ascendentes de infraestructuras (*upstream*), y corresponden al escenario hipotético 5: de interrupción de servicios públicos, lo que provoca efectos en cadena.

Nota: el acceso de las entidades financieras a los servicios electrónicos Sebra que ofrece el Banco de la República (Banrep) puede hacerse por: 1) canal de comunicaciones dedicado, punto a punto, entre sus instalaciones y el Banrep, o 2) a través de internet.
Fuente: https://www.banrep.gov.co/sites/default/files/paginas/reque_tecnico_conex_sebra.pdf.

Datos: para el ejercicio de simulación se tomaron las transacciones de los diez días de mayor valor de pagos que ocurrieron durante 2023 entre las 7:00 *a. m.* y 9:00 *p. m.* en el CUD. Se excluyen las transacciones realizadas entre el Banrep, la Dirección General de Crédito Público y del Tesoro Nacional y el Sistema General de Regalías.

Escenario de referencia: este considera las transacciones observadas que fueron liquidadas, una a una, en la secuencia en que se dieron bajo la modalidad de liquidación bruta en tiempo real (LBTR) con los saldos de inicio de día disponibles en cuentas de depósito de sus participantes durante las fechas seleccionadas. El valor y número de los pagos exitosamente liquidados en este escenario se constituye en la base de comparación para medir el impacto de un ciberataque en los escenarios formulados antes.

Forma de reaccionar de los participantes: los escenarios de ciberataque descritos se elaboran considerando que, por operatividad del SPAV, las contrapartes, al desconocer la identidad de la entidad atacada (quien es la sometida al ciberataque y deja de enviar pagos), reaccionan de forma diferente en el envío de los pagos. De modo que, ante la insuficiencia de saldo ocasionada por los incumplimientos de la entidad atacada, estas contrapartes intentan cumplir con los pagos en la secuencia del escenario de referencia, pero si estos no logran ser exitosamente liquidados, su reacción para reintentar la liquidación puede ser pasiva o activa.

En la reacción pasiva, las entidades afectadas (EA), o sea, aquellas con operaciones que no pudieron liquidar al primer intento, como ocurrió en el escenario de referencia, no reintentarían liquidarlas y se acumularían en un lote de operaciones incumplidas. De este modo la liquidez de estos pagos incumplidos no llegaría a sus entidades destinatarias y determinaría el tamaño de la cadena de incumplimientos y del número de EA en el sistema.

Por su parte, en la reacción activa las contrapartes almacenan en una cola de espera las operaciones que inicialmente no pudieron ser liquidadas y, en la medida en que ingresan recursos a su cuenta por pagos entrantes, tratan de liquidar sus pagos pendientes en cola empleando un algoritmo *FIFO* (*first in – first out*). Aunque en esta forma de reacción es viable suponer también el desconocimiento de la identidad de la EA, la reacción de las contrapartes hace que la liquidez sea manejada de forma más eficiente y que los impactos en el valor de los pagos y el número de entidades afectadas sean menores al resultante bajo una reacción pasiva.

Bajo cada escenario se realizaron simulaciones donde las entidades reaccionaron de forma pasiva o activa ante los incumplimientos de la entidad atacada, con el objetivo de evaluar el impacto potencial del ciberataque en términos del valor y número de pagos incumplidos y el número de entidades afectadas.

3. Resultados

3.1 Ciberataque simultáneo a entidades sistémicamente importantes

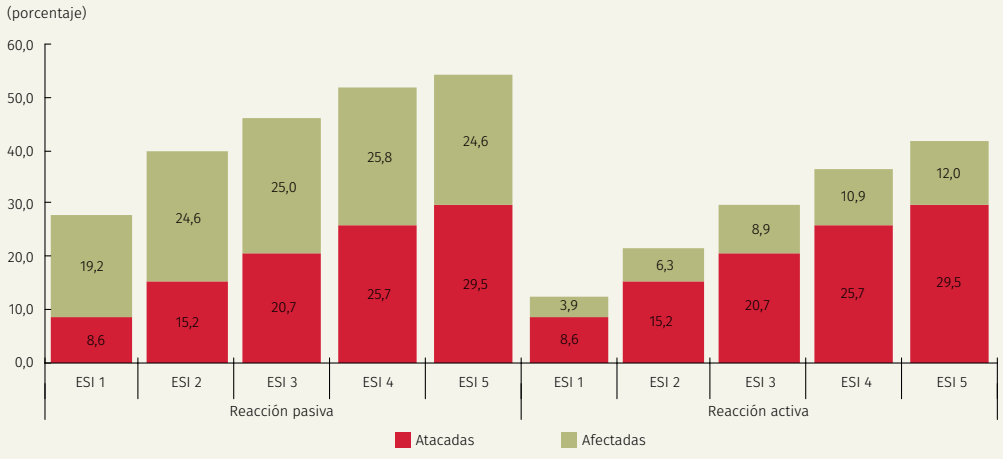
El ejercicio de simulación se realiza, como lo hacen Eisenbach, Kovner y Lee (2022a) para Fedwire, dirigiendo ataques cibernéticos a hasta cinco entidades sistémicamente importantes (ESI) al mismo tiempo.

El criterio de selección de las ESI sometidas a ciberataque para cada uno de los días considerados corresponde al elaborado por el DSIF para hacer el monitoreo del CUD. Lo anterior, basado en un escalafón de importancia calculado mediante un análisis de componentes principales donde se incluyen variables como cantidad y monto de operaciones realizadas, número de contrapartes, así como el papel que como distribuidor o receptor de pagos pueda tener cada entidad participante del CUD.

En el Gráfico R1.1 se muestran los porcentajes del valor de los pagos que con respecto al escenario de referencia dejaron de liquidarse, tanto por las ESI sometidas a ciberataques simulados, como por aquellas afectadas que no pudieron cumplir con todas sus obligaciones de pago cuando se asume tanto una reacción pasiva como una activa.

En dicho gráfico se aprecia que cuando se asume una reacción pasiva, el valor promedio de los pagos incumplidos, medidos como porcentaje del valor liquidado en los días seleccionados, para las ESI atacadas se ubica entre 8,6 % cuando se trata de la principal ESI atacada, hasta 29,5 % cuando los ciberataques se dirigen al mismo tiempo a las cinco ESI

Gráfico R1.1
Valor de los incumplimientos como porcentaje del escenario de referencia: reacciones pasiva y activa



Fuente: Banco de la República (DSIF)

más importantes. Simultáneamente, y en la misma unidad de medida, el porcentaje promedio de incumplimientos de las entidades afectadas fluctuó entre un mínimo de 19,2 %, cuando el ciberataque ocurrió a la principal ESI, y un máximo de 25,8 %, cuando el ataque se dirigió a cuatro ESI.

Cuando se considera que las entidades afectadas asumen una reacción activa, utilizando la liquidez que les suministran sus contrapartes para reintentar la liquidación de sus pagos incumplidos, el impacto sobre el sistema se reduce de manera importante. En el Gráfico R1.1 es posible apreciar que, como el ciberataque tanto en la simulación con reacción pasiva y activa se dirige a las mismas ESI, el valor de los incumplimientos es el mismo, pero los de las entidades afectadas se reducen dado el uso más eficiente de la liquidez.

En efecto, en el Gráfico R1.1 también se observa que, bajo reacción activa, el porcentaje del valor de incumplimientos de las entidades afectadas se reduce con relación al de reacción pasiva. En este caso el porcentaje promedio del valor de los incumplimientos, respecto al escenario de referencia, es del 3,9 % cuando la principal ESI no puede enviar pagos y del 12,0 % en el caso extremo de un ataque a cinco ESI.

El mismo Gráfico R1.1 muestra que los valores de los incumplimientos, medidos como porcentaje de los pagos observados (escenario de referencia), aumentan a medida que se amplía el número de ESI sometidas a ciberataques, independiente de la reacción que se asuma. También refleja que mientras que los pagos incumplidos de las entidades atacadas son los mismos, el valor total de los incumplimientos (entidades atacadas y afectadas) en el caso de la reacción activa es del 12,4 % si se trata del ataque a una ESI y del 41,5 % si son cinco ESI. Cuando en la simulación se asume una reacción pasiva, el valor total de los pagos incumplidos aumenta ante el ciberataque a una ESI al 27,7 % y al 54,1 % cuando es a cinco ESI.

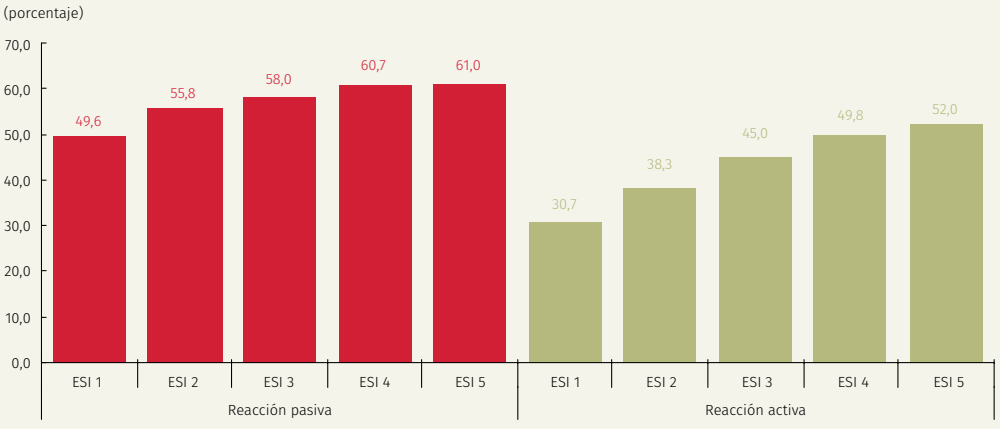
Cuando se cuantifica el impacto por el número de entidades afectadas con relación a las activas, se aprecia en el Gráfico R1.2 que al asumir una reacción pasiva en todos los ciberataques (de una ESI hasta cinco ESI) se afecta a más de la mitad (50 %) de las entidades activas, y en el caso extremo de cinco ESI el porcentaje alcanza a ser del 61,0 %. Bajo una reacción activa, el mismo indicador se reduce al 30,7 % para el ciberataque de una ESI y solo en el caso de cinco ESI termina afectada un poco más de la mitad de las entidades activas (52,0 %).

3.2 Ciberataque a proveedores de comunicaciones

Los ciberataques a proveedores de servicios de una infraestructura o de sus clientes se catalogan como ataques contracorriente o *upstream*, y sus efectos en cadena pueden incluso llegar a impactar al sector financiero y la economía.

El sector financiero, dentro del que se cuentan las infraestructuras críticas de un país, dependen de la electricidad y del funcionamiento adecuado de las telecomunicaciones y de la tecnología. Interrupciones prolongadas en el funcionamiento de estos proveedores

Gráfico R1.2
Porcentaje promedio de entidades afectadas respecto al total de activas: reacciones pasiva y activa



Fuente: Banco de la República (DSIF)

pueden afectar la capacidad de funcionamiento y prestación de servicios de la infraestructura y de sus participantes.

Una de las recomendaciones técnicas que el Banrep realiza para acceder a los servicios electrónicos que presta[2], como es el caso del CUD, es que sus participantes mantengan canales alternos independientes con un proveedor diferente para su conexión. De esta forma, en caso de una contingencia en la que el canal dedicado principal deja de funcionar, ya sea por una falla operativa o un ciberataque, la pronta conmutación al canal alterno le permitiría a la entidad restituir su conexión y servicio a la mayor brevedad.

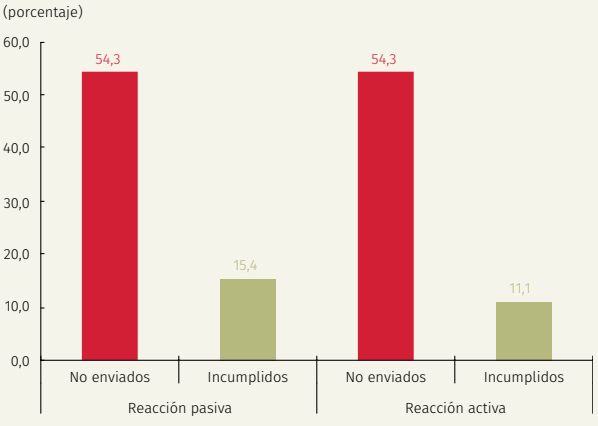
En la medida en que exista una alta concentración de los participantes de un sistema de pagos en un solo proveedor de telecomunicaciones, mayor será el impacto que ocasionaría un ciberataque dirigido a este. Esta situación podría agravarse si las entidades no cumplen con la recomendación de tener habilitada una segunda línea.

Los ciberataques simulados que aquí se elaboran suponen que las entidades que se conectan al CUD con el principal o el segundo proveedor de telecomunicaciones no tienen habilitada la segunda línea dedicada y, por tanto, al perder su conexión, no pueden enviar pagos.

En el Gráfico R1.3 se observa que, como efecto de ciberataque al principal proveedor de telecomunicaciones, el porcentaje del valor de los pagos no liquidados respecto a los observados en el escenario de referencia cae en promedio un 54,3 % por la desconexión de sus clientes. Adicionalmente, como efecto de segunda vuelta, el incumplimiento de las entidades afectadas sería del 15,4 % frente a una reacción pasiva y del 11,1 % ante una activa. La ausencia de un canal alterno, que se asume en este ejercicio extremo pero plausible, haría que el impacto potencial de ataques a terceros críticos sea exacerbado ocasionando disrupciones importantes en el CUD.

En el Gráfico R1.4 se aprecia que el ciberataque al principal proveedor de conexión al CUD generaría un impacto importante a la liquidación, haciendo que el valor total de los incumplimientos[3] ascienda al 69,7 %

Gráfico R1.3
Valor de los incumplimientos por ciberataque al principal proveedor de telecomunicaciones (como porcentaje del escenario de referencia)



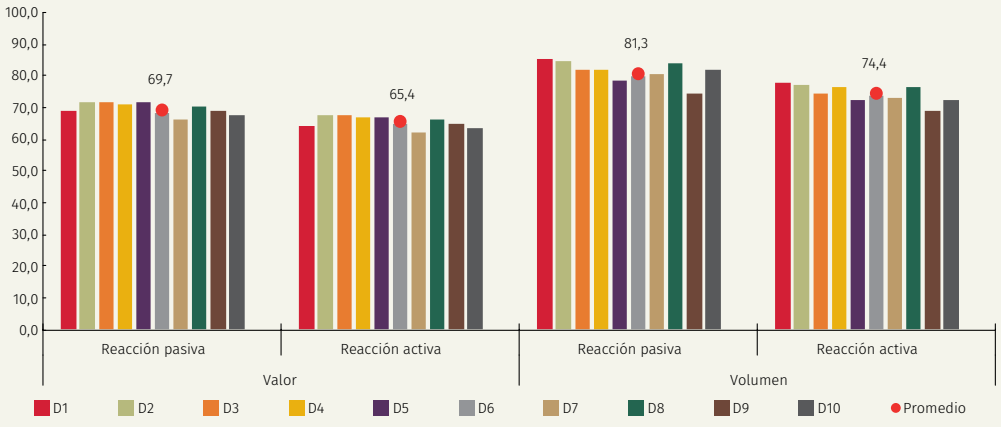
Fuente: Banco de la República (DSIF)

2 "Requerimientos técnicos para los servicios electrónicos del Banrep Sebra", mayo de 2024, disponible en: https://www.banrep.gov.co/sites/default/files/paginas/reque_tecnico_conex_sebra.pdf

3 Tanto por efecto directo, por los pagos que dejan de enviar las entidades que resultan desconectadas, como efecto de segunda vuelta, por los pagos cuyas contrapartes tienen un proveedor diferente, dejan de realizarlos debido a la liquidez no recibida.

Gráfico R1.4
Valor y volumen de los pagos incumplidos ante el ciberataque al principal proveedor de telecomunicaciones

(como porcentaje de los pagos observados en el escenario de referencia)



Fuente: Banco de la República (DSIF)

en el caso de reacción pasiva y que solo se reduzca marginalmente al 65,4 % cuando las entidades sobrevivientes reaccionan activamente. Respecto al número de transacciones, el ciberataque provocaría que el 81,3 % del total de las observadas en el escenario de referencia no pudieran ser liquidadas en el caso de reacción pasiva y del 74,4 % con una activa.

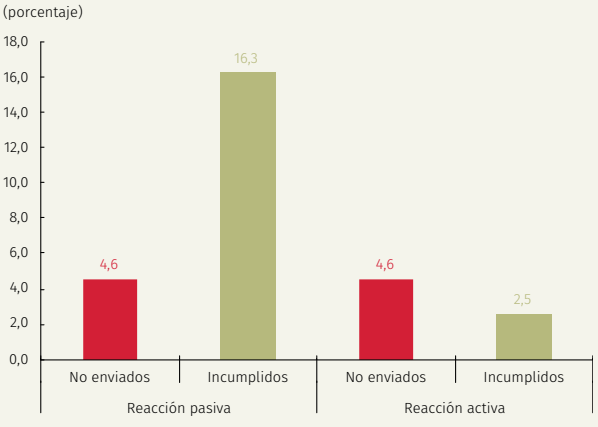
Una explicación del resultado anterior es la alta concentración que tienen los participantes del CUD en el principal proveedor de telecomunicaciones, ya que, como se observa en el Cuadro R1.2 más de la mitad de las entidades activas quedarían desconectadas si este proveedor experimentara un ciberataque, impidiendo a sus clientes enviar pagos. Además,

Cuadro R1.2
Porcentaje de entidades activas y afectadas posciberataque al principal proveedor de telecomunicaciones al CUD: reacciones pasiva y activa

Día	Activas posciberataque	Reacción pasiva Afectadas	Reacción activa Afectadas
	Como porcentaje de las entidades activas en escenario de referencia	Como porcentaje de las activas posciberataque	
D1	50,8 %	68,9 %	65,6 %
D2	51,2 %	68,3 %	65,1 %
D3	51,6 %	68,8 %	68,8 %
D4	50,8 %	66,1 %	64,5 %
D5	50,8 %	64,5 %	64,5 %
D6	52,8 %	59,1 %	59,1 %
D7	51,6 %	60,9 %	60,9 %
D8	52,4 %	67,7 %	67,7 %
D9	53,5 %	55,1 %	55,1 %
D10	52,8 %	59,1 %	59,1 %
Promedio	51,8 %	64,2 %	63,4 %

Fuente: Banco de la República (DSIF).

Gráfico R1.5
Valor de los incumplimientos por ciberataque al segundo principal proveedor de telecomunicaciones
(como porcentaje del escenario de referencia)



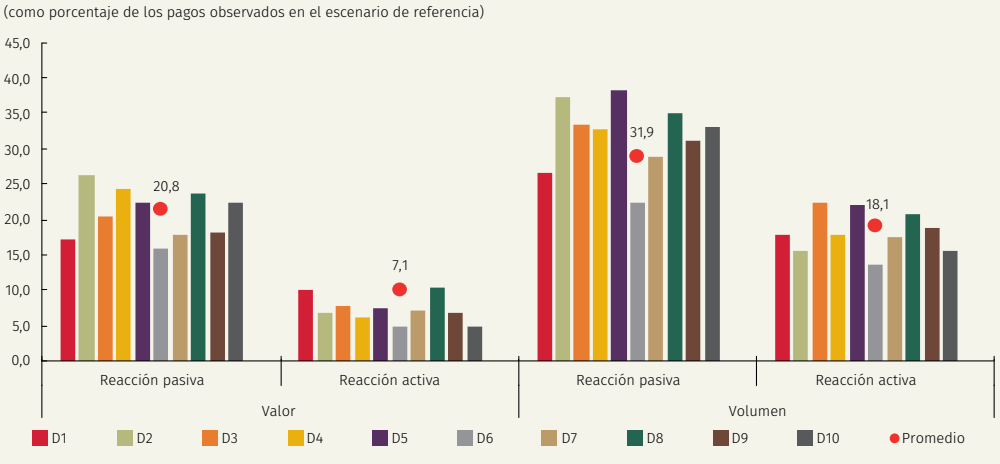
Fuente: Banco de la República (DSIF)

la liquidez no provista por las entidades desconectadas ocasionaría que, de las entidades sobrevivientes (cuya conexión al sistema se establece con otro proveedor), dos terceras partes acabarían afectadas, con pagos no liquidados.

Cuando se realiza el ciberataque al segundo principal proveedor de telecomunicaciones, que respecto al principal proveedor permite la conexión de un menor número de participantes al CUD, se puede apreciar que el impacto en el valor y volumen de los pagos incumplidos es menor que el del principal. En efecto, las entidades desconectadas dejarían de enviar en promedio un 4,6 % de los pagos del escenario de referencia y que, por efecto de segunda vuelta, las entidades afectadas dejarían de liquidar 16,3 % de los pagos asumiendo una reacción pasiva y 2,5 % bajo una activa (Gráfico R1.5).

El Gráfico R1.6 muestra que los incumplimientos totales diarios y en promedio, tanto en valor como en volumen, con la reacción activa atenúan al impacto del ciberataque frente a la pasiva. En efecto, mientras que en la reacción pasiva el porcentaje de incumplimientos respecto al escenario de referencia es del 20,8 % en valor y 31,9 % en volumen, bajo una reacción activa estos descienden al 7,1 % y 18,1 %, respectivamente.

Gráfico R1.6
Valor y volumen de los pagos incumplidos ante el ciberataque al segundo principal proveedor de telecomunicaciones



Fuente: Banco de la República (DSIF)

Reconociendo que, dado que aquí el número de participantes que se conectan al CUD es menor que el del principal proveedor, el impacto directo e indirecto de incumplimientos que se genera también lo es. Según el Cuadro R1.3, más del 84 % de las entidades seguirían activas y enviarían sus pagos, pero el 16 % dejaría de hacerlo, ocasionando incumplimientos por parte del 54 % de las entidades en la reacción pasiva y del 37,3 % en la activa.

Ante estos resultados, es recomendable fortalecer la resiliencia de las entidades ante la interrupción de operaciones como consecuencia de los ataques cibernéticos aquí simulados.

Cuadro R1.3
Porcentaje de entidades activas y afectadas posciberataque al segundo principal proveedor de telecomunicaciones al CUD: reacciones pasiva y activa

Día	Activas posciberataque	Reacción pasiva Afectadas	Reacción activa Afectadas
	Como porcentaje de las entidades activas en escenario de referencia	Como porcentaje de las activas posciberataque	
D1	85,0 %	52,9 %	39,2 %
D2	84,6 %	57,7 %	39,4 %
D3	83,9 %	51,9 %	40,4 %
D4	84,4 %	59,2 %	36,9 %
D5	84,4 %	54,4 %	38,8 %
D6	84,8 %	45,3 %	33,0 %
D7	83,9 %	51,0 %	36,5 %
D8	83,9 %	54,8 %	40,4 %
D9	84,5 %	45,9 %	35,8 %
D10	84,8 %	51,9 %	33,0 %
Promedio	84,4 %	52,4 %	37,3 %

Fuente: Banco de la República (DSIF).

Diagrama R1.1
Mecanismos y políticas de mitigación

- Marco regulatorio y políticas de mitigación
- Educación y entrenamiento continuo
- Adopción de IA generativa como mecanismo de mitigación
- Cooperación internacional
- Simulación y análisis de escenarios

Fuente: Banco de la República (DSIF)

4. Mecanismos y políticas de mitigación

El sector financiero, debido a su interconexión y dependencia de proveedores de telecomunicaciones, se enfrenta a un riesgo cibernético creciente. La ciberseguridad, además de ser una preocupación técnica, se constituye en una prioridad estratégica esencial para garantizar la estabilidad y resiliencia del sistema financiero global. Como se presentó en el *Reporte de Infraestructuras Financieras* (2023), la implementación de políticas robustas y recomendaciones estratégicas es vital para mitigar este riesgo y su potencial impacto sistémico. Dentro de los mecanismos y políticas identificadas para mitigar el riesgo cibernético y su potencial impacto sistémico se encuentran (véase el Diagrama R1.1).

- Marco regulatorio y políticas de mitigación: un marco regulatorio sólido es crucial para mitigar el riesgo cibernético en el sector financiero. Diversos estudios subrayan la importancia de desarrollar y fortalecer marcos regulatorios que promuevan mejores prácticas de seguridad cibernética y se adapten a las dinámicas cambiantes de amenazas y tecnologías. Además, es fundamental fomentar la cooperación entre el sector público y privado y armonizar los estándares internacionales para mejorar la seguridad cibernética global (Bank of England, 2018; BIS, 2020; Warren, Kaivanto y Prince, 2018; Aldasoro, Gambacorta, Giudici y Leach, 2020).
- Educación y entrenamiento continuo: la capacitación continua del personal en ciberseguridad es esencial para fortalecer la primera línea de defensa contra ataques cibernéticos. Es necesario mantener al personal actualizado sobre las últimas amenazas y tácticas de mitigación mediante simulacros regulares y programas de concienciación. Esto asegura que los empleados estén preparados para identificar y responder adecuadamente a intentos de ciberataque (Zurich, 2014).
- Simulación y análisis de escenarios: la realización de simulaciones y análisis de escenarios constituye una herramienta crítica

para evaluar la preparación y resiliencia de las instituciones financieras. Las simulaciones de ciberataques coordinados permiten identificar vulnerabilidades sistémicas y desarrollar estrategias de mitigación específicas. Estos ejercicios destacan la necesidad de contar con planes de continuidad de negocios y recuperación de desastres que sean robustos y efectivos (Kaffenberger y Kopp, 2019; Eisenbach, Kovner y Lee, 2022b).

- Cooperación internacional: la cooperación internacional es fundamental para gestionar el riesgo cibernético, ya que los ciberataques traspasan fronteras. La posibilidad de compartir inteligencia sobre amenazas y coordinar estrategias de respuesta a nivel global mejoran significativamente la capacidad de respuesta ante ciberataques y aseguran una defensa más robusta contra amenazas globales (Aldasoro *et al.*, 2021; BIS, 2020).

- Adopción de IA generativa como mecanismo de mitigación: la IA generativa (IA gen) comprende las tecnologías de inteligencia artificial que, basadas en datos de entrenamiento, pueden generar contenido nuevo y diverso. La IA introduce tanto oportunidades como retos[4] en la administración del riesgo cibernético en el sistema financiero, incluidos los bancos centrales (Aldasoro *et al.*, 2024).

  En el ámbito de la ciberseguridad la IA gen emerge como un mecanismo adicional para mitigar el riesgo cibernético y su impacto sistémico. Dentro de las posibilidades que Aldasoro *et al*. (2024) identifican que ofrece la IA gen respecto a la ciberseguridad están: 1) la mejora en la detección de amenazas; 2) la automatización de tareas rutinarias en ciberseguridad; 3) su respuesta rápida y eficiente mejora la capacidad de respuesta a ciberataques; 4) el aprendizaje continuo y adaptación de los sistemas de IA gen a amenazas emergentes; 5) la reducción de la probabilidad de errores humanos en la gestión de amenazas cibernéticas; 6) la posibilidad de creación de perfiles de comportamiento y riesgo personalizados mejora la precisión de las medidas de seguridad, y 7) facilita la anticipación de posibles amenazas y su neutralización antes de que se materialicen (Diagrama R1.1).

En síntesis, la integración de la IA gen en las estrategias de ciberseguridad no solo fortalece las capacidades existentes, sino que también introduce nuevas formas de gestionar y mitigar el riesgo cibernético, reduciendo su impacto potencial en el sistema financiero y mejorando la resiliencia sistémica.

5. Conclusiones

- El ente supervisor puede promover que los participantes del CUD, y en especial aquellas entidades que jueguen un rol relevante en dicha infraestructura, mantengan sistemas de ciberseguridad lo suficientemente robustos para reducir su vulnerabilidad a ataques cibernéticos y mitigar así, el potencial impacto negativo de incumplimiento de pagos que se generaría en el sistema, dada la interconectividad de los pagos.

- Continuar fomentando que los participantes del CUD cuenten con dos canales alternos dedicados independientes con diferentes proveedores para garantizar que, en caso de falla del principal, se logre una rápida recuperación de la conexión y operación, mediante la pronta conmutación al canal alterno. Un mecanismo que podría ser considerado por la industria y que contribuiría a mitigar el impacto que sobre la liquidez del sistema ocasionaría un ciberataque a los proveedores de comunicaciones es propender por moderados niveles de concentración en estos. El impacto negativo de este tipo de ataque podría exacerbarse si los participantes no disponen de un canal alterno y se conectan al sistema únicamente mediante el proveedor de alta concentración.

- Frente a la forma como reaccionan las entidades ante el incumplimiento de pagos de sus contrapartes, las simulaciones realizadas permiten validar el efecto mitigador que se obtiene por la mayor eficiencia en el uso de la liquidez al reintentar en el cumplimiento de pagos al asumir una reacción activa. Los resultados obtenidos bajo estos supuestos en las simulaciones buscan crear conciencia a nivel de participantes sobre la forma en la que pueden reaccionar las entidades ante incumplimientos de pagos de sus contrapartes.

---

4 Aldasoro *et al*. (2024) identifica que con la sofisticación de las herramientas IA gen y su uso ampliado, la frecuencia, velocidad y complejidad de los ciberataques se incrementa. Dentro de las amenazas especificas asociadas a la IA gen se incluyen la ingeniería social, ataques día cero y ataques *malware* para la infiltración de datos.

- Las infraestructuras financieras son esenciales para el funcionamiento adecuado del sistema financiero. La prestación de sus servicios depende en gran medida de un alto componente tecnológico, lo que las hace particularmente vulnerables a los ciberataques. Resulta importante contar con una buena coordinación entre la industria y el ente supervisor para implementar marcos de ciberresiliencia robustos y planes de respuesta y recuperación bien definidos para garantizar la continuidad de los servicios críticos durante y después de un ataque (IMF, 2024).

- La ciberseguridad también juega un papel fundamental en la estabilidad financiera, ya que ataques de tipo cibernético pueden resultar en pérdidas financieras directas y de confianza en el sistema financiero, lo que podría provocar retiros masivos de depósitos, liquidación de activos y reacciones adversas en el mercado. Medidas tendientes a facilitar la aplicación de una estrategia nacional de ciberseguridad, una regulación efectiva, una supervisión adecuada en este riesgo, así como la consolidación de una fuerza de trabajo en ciberseguridad, la instauración de unos acuerdos nacionales e internacionales de intercambio de información, junto con la cooperación internacional, fortalecerían la ciberresiliencia del sector financiero (IMF, 2024).

- Incorporar un componente de ciberseguridad en los indicadores de liquidez permitiría que las entidades financieras evaluaran mejor su capacidad de respuesta ante incidentes cibernéticos para asegurar la continuidad de sus operaciones, contribuyendo de esta forma a la estabilidad financiera. En esta línea la propuesta práctica del IMF (2024) para evaluar el posible efecto de incidentes cibernéticos en la posición de liquidez de los bancos, consiste en calcular la tasa de retiro de depósitos a la cual el índice de cobertura de liquidez se ubicaría por debajo del requisito regulatorio del 100%.

Referencias

Aldasoro, I.; Doerr, S.; Gambacorta, L.; Notra, S.; Oliviero, T.; Whyte, D. (2024). "Generative Artificial Intelligence and Cyber Security in Central Banking", *BIS Paper*, núm. 145 (mayo), Bank for International Settlements.

Aldasoro, I.; Frost, J.; Gambacorta, L.; Whyte, D. (2021). "Cyber Risk in the Financial Sector", Bank for International Settlements.

Aldasoro, I.; Gambacorta, L.; Giudici, P.; Leach, T. (2020). "Operational and Cyber Risks in the Financial Sector", Bank for International Settlements.

Atlantic Council (2016). "Understanding Systemic Cyber Risk", Global Agenda Council on Risk and Resilience,World Economic Forum (WEF), *White Paper* (octubre)

Bank of England (2018). "The Bank's Approach to Operational Resilience".

Bank of International Settlements [BIS] (2020). "Principles for Operational Resilience and Cyber Risk", Bank for International Settlements.

Banco de la República (2023). "Recuadro 4: Altos niveles de ciberresiliencia como factor clave para la estabilidad de las infraestructuras financieras", *Reporte de la Infraestructura Financiera*, Departamento de Seguimiento a la Infraestructura Financiera (DSIF).

Eisenbach, T. M.; Kovner, A.; Lee, M. J. (2022a) "Cyber Risk and the U.S. Financial System: A pre-Mortem Analysis", *Journal of Financial Economics*, vol. 145, núm. 3.

Eisenbach, T. M.; Kovner, A.; Lee, M. J. (2022b). "When it Rains, It Pours: Cyber Risk and Financial Conditions", Staff Reports, núm. 1022/June, Federal Reserve Bank of New York.

International Monetary Fund [IMF] (2024) "Cyber risk: a growing concern for macro-financial stability" – Global financial stability report: The Last Mile: Financial Vulnerabilities and Risks. Chapter 3, International Monetary Fund. (April)

Kaffenberger, L.; Koop, E. (2019). "Cyber Risk Scenarios, the Financial Systems and Systemic Risk Assessment", Cyber Policy Initiative Working Paper Series *Cybersecurity and the financial systems*, núm. 4, septiembre, Carnegie Endowment for International Peace.

Warren, G.; Kaivanto, K.; Prince, D. (2018). "Could a cyber-attack cause a systemic impact in the financial sector?", *Quarterly Bulletin*. Bank of England. (2018 Q4)

Zurich (2014). "Beyond Data Breaches: Global Interconnections of Cyber Risk", *Risk Nexus* (abril).