REPORTE QUINCENAL

17-31 de julio 2021

En el 2do trimestre, el PIB vuelve a su crecimiento histórico de 1.5% mensual

Macro

Se muestra el crecimiento del PIB observado en el 2do trimestre, además se analiza el efecto de la pandemia en el mercado laboral y su recuperación ligada a la de la economía.

Seguros

Se presenta la densidad del seguro, como un indicador para poder identificar las brechas del seguro tano en género y edad, para vida, gastos médicos, accidentes personales y pensiones

Tema de Análisis

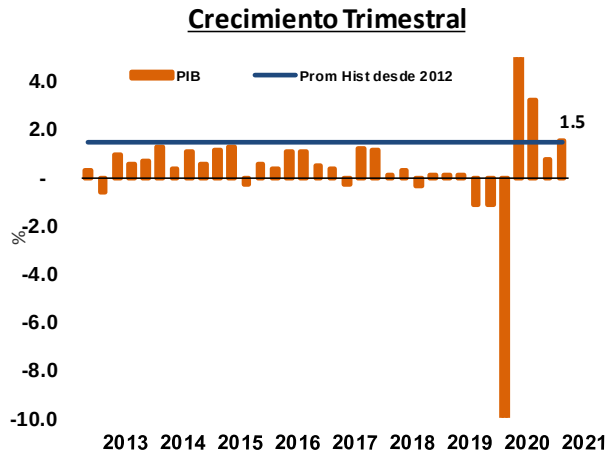
La ciberseguridad, las ciberamenazas y los hackers se escuchan cada vez con mayor frecuencia y son parte de las noticias nacionales e internacionales en el día a día. Con base en lo anterior, se considera importante una reflexión sobre este tema y, dada su relevancia, en esta ocasión incluimos los aspectos más importantes de su artículo en el boletín quincenal.

COYUNTURA MACRO

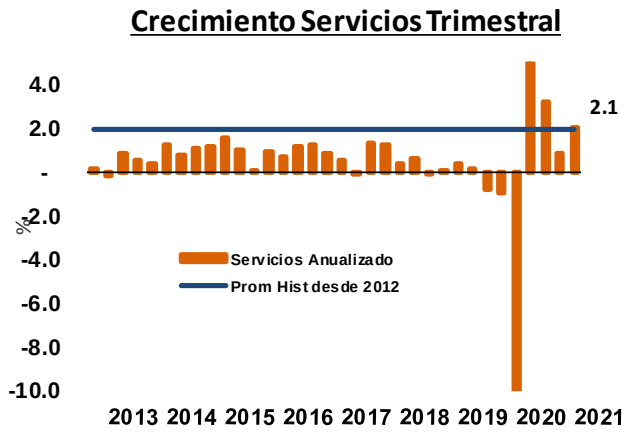
Crecimiento. En el 2do trimestre el PIB creció 1.5% respecto al mes anterior, lo cuál es el mismo nivel que el promedio histórico calculado desde 2012, este crecimiento fue impulsado por el sector servicios con un aumento de 2.1%, mientras que el sector industrial sigue mostrando poca dinámica en su recuperación con un crecimiento de a penas 0.43%.

La encuesta de expectativas del sector privado de Banxico muestra un ligero aumento en la velocidad de la recuperación, dado que en julio el pronóstico de crecimiento para 2021 aumentó a 6.06% lo que significa un aumento de 0.26% respecto a lo esperado en junio.

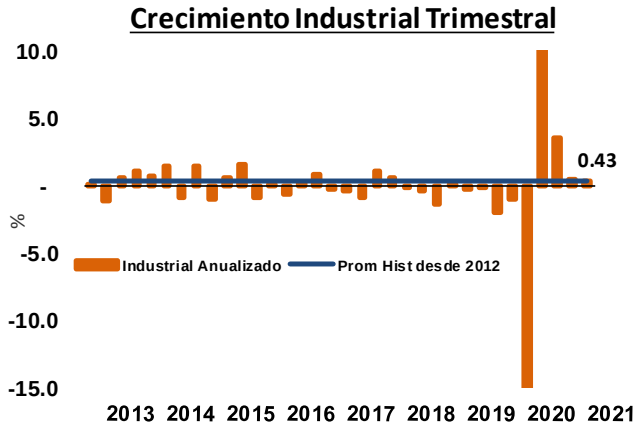
El PIB en el 2doT creció 1.5%, esto debido…



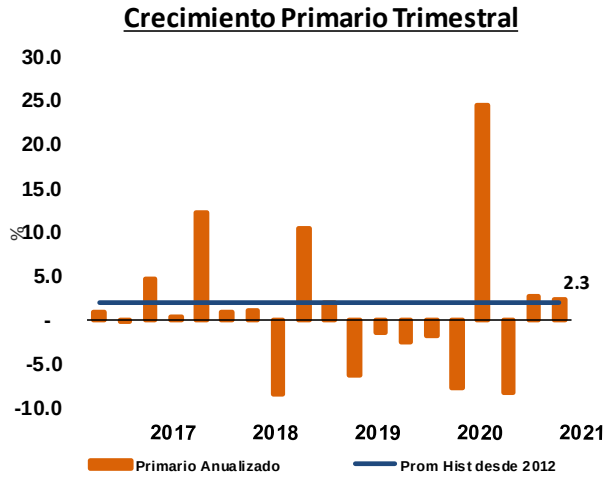
al crecimiento de 2.1% en el sector servicios,…



a un crecimiento de 0.43% en el sector industrial y…



de 2.3% en el sector primario.



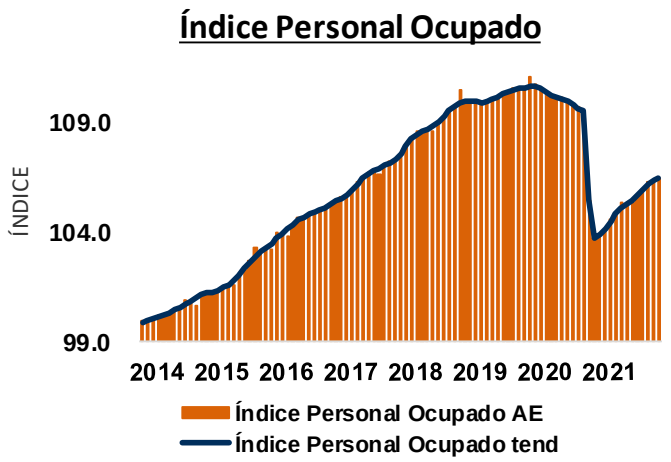
Fuente: INEGI

COYUNTURA MACRO

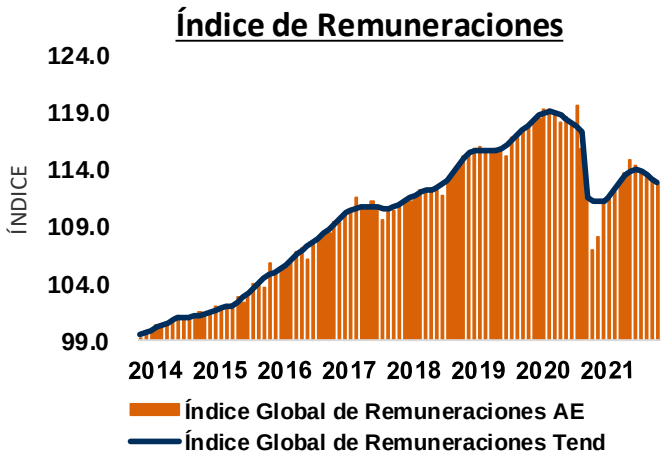
Personal Ocupado. El índice de personal ocupado todavía se encuentra lejos de los niveles pre pandemia, esto debido a que la recuperación de la economía no alcanza la dinámica suficiente para generar los empleos que se perdieron a causa del cierre de la economía. Esto se ve con las tasas de crecimiento mensual del índice, las cuales muestran crecimientos decrecientes (marzo 0.37%, abril 0.07%, mayo 0.06%).

Remuneraciones. Tanto el índice las remuneraciones, como el de las remuneraciones medias muestran una clara tendencia a la baja, y el primero se encuentran en un nivel muy inferior al pre pandémico. Esta caída en la calidad del empleo se explica por la pérdida de ahorro de la economía, que implica una menor inversión y por ende una menor productividad la cual determina el nivel de remuneraciones.

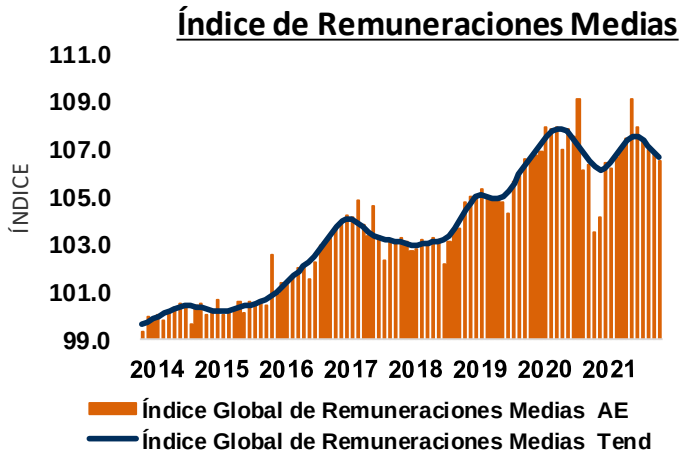
El índice de personal ocupado en mayo creció 0.06% respecto al mes anterior…



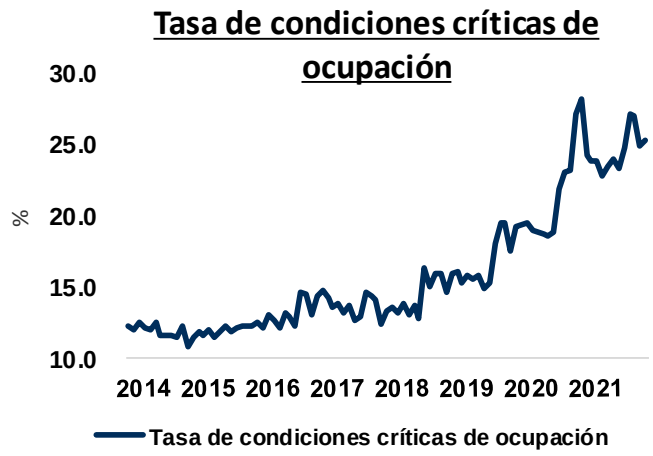
y las remuneraciones muestran una preocupante deterioro,…



lo que lleva a la tendencia remuneraciones medias a la baja.



Esto ha aumentado de forma importante la tasa de ocupación en condiciones críticas, que en junio se encontró en 25.5%.



Fuente: INEGI

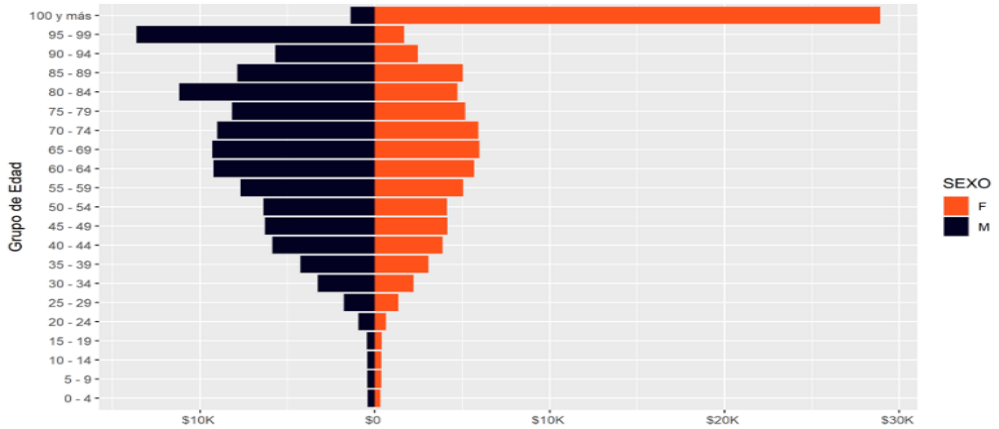
COYUNTURA SEGUROS

Densidad del seguro por edad y sexo: La penetración de los seguros es un fenómeno multifactorial, caracterizado por factores tales como edad, sexo, nivel de ingreso, educación y tipo de seguro. Si bien la penetración es una de las herramientas más sencillas para evaluar el desarrollo de un mercado de seguros, no debe ser el único parámetro a tomar en cuenta pues no brinda información acerca de las brechas de seguros.

Desarrollar políticas públicas desde un entendimiento integral del sector es necesario para poder evaluar el impacto de estas, por ello además de tomar en cuenta la penetración del seguro es necesario tomar en cuenta otros indicadores como la **densidad del seguro** que mide la prima por habitante, permite conocer como la estructura demográfica afecta al seguro.

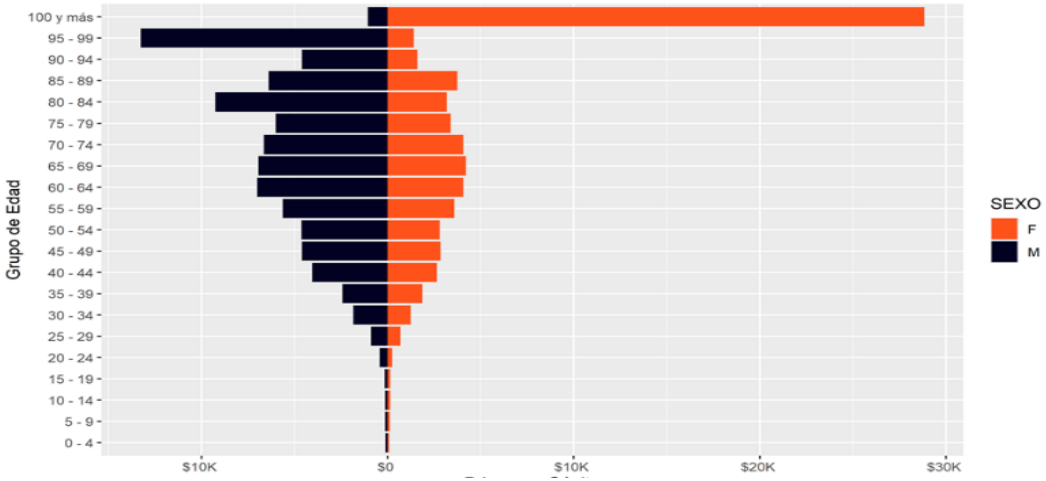
La densidad por prima del Sector[1] se ubicó durante 2020 en $2,886, se observa una mayor pago de prima en las edades más altas, asociado con el aumento de la mortalidad, la densidad promedio total es 43% superior en hombres respecto a las mujeres.

Distribución de la densidad del sector por rango de edad



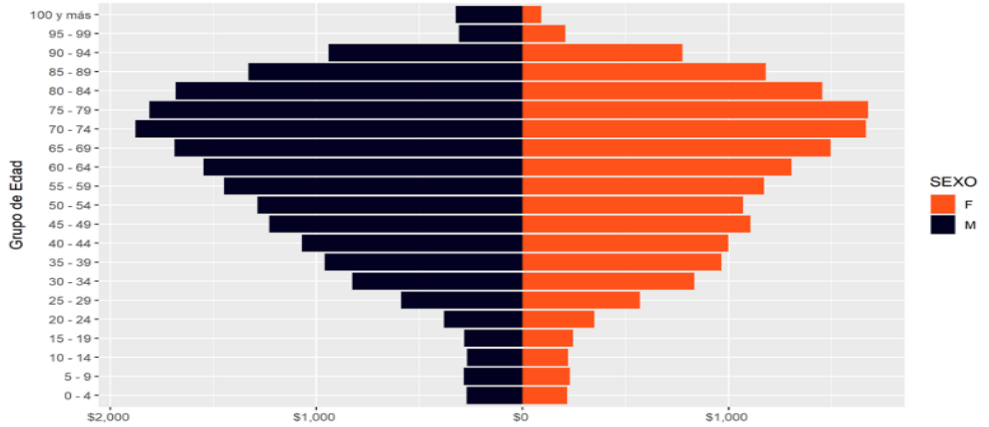
Vida. Muestra un comportamiento similar al del mercado, se observa que a partir de los 20 años aumenta la densidad del seguro, para continuar el crecimiento hasta los 64 años. La densidad promedio total en hombres es 51% superior a la observada de las mujeres.

Distribución de la densidad por rango de edad, Vida



Gastos Médicos. La densidad se concentra en edades altas teniendo su máximo en el rango de 70 a 74 años, la densidad promedio total en hombres es 7.5% superior a la observada en mujeres.

Distribución de la densidad por rango de edad, Gastos Médicos

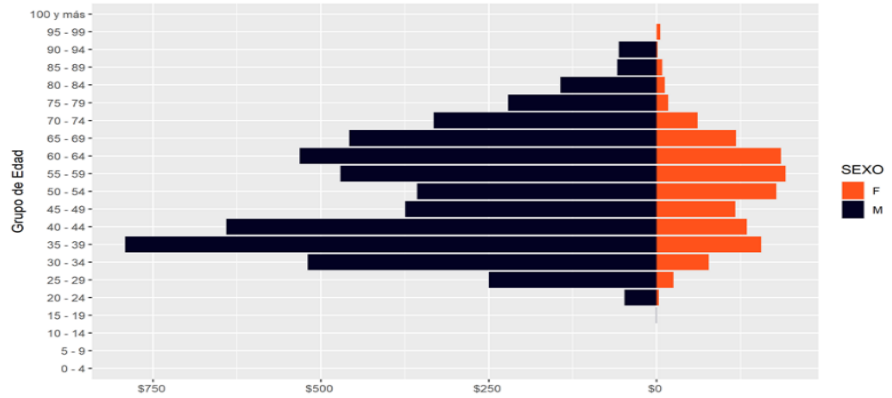


1. Para este análisis se consideran las operaciones de Vida, Pensiones Accidentes y Enfermedades

Fuente: CNSF

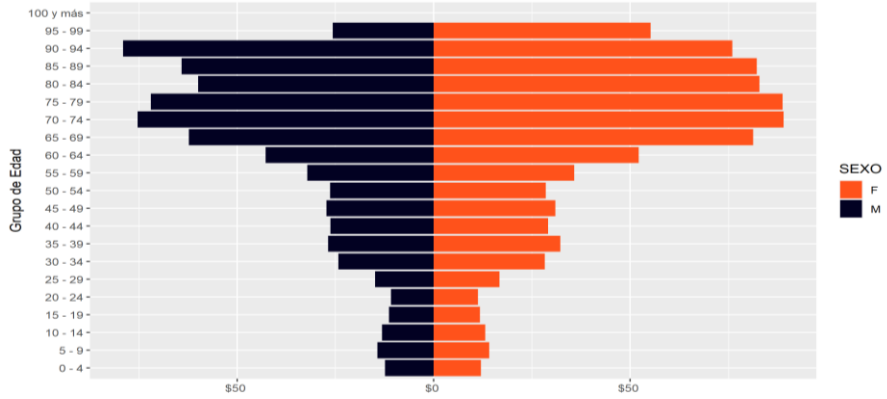
Pensiones. La densidad se ve afectada por la transición entre sistemas de seguridad social, concentrando la mayor densidad en pensiones para hombres de 35 a 39 años causadas principalmente por invalidez e incapacidad, la densidad promedio del seguro en pensiones **es el triple en hombres respecto a las mujeres.**

Distribución de la densidad por rango de edad, Pensiones



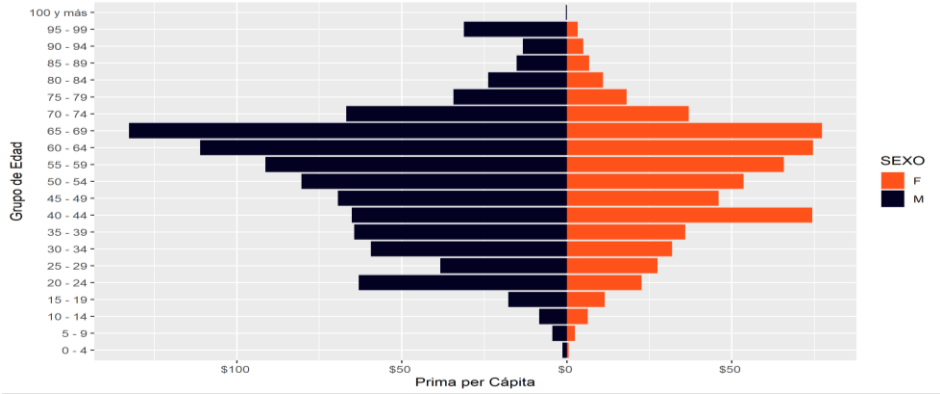
Salud. La densidad aumenta en las edades más avanzadas de los asegurados, concentrándose en los grupos de edad de 65 años en adelante. A diferencia del resto del sector, en estos seguros la densidad de la prima es mayor en las mujeres que superan en 18.2% a los hombres.

Distribución de la densidad por rango de edad, Salud



Accidentes Personales. La densidad se concentra en el rango de 50 a 69 años, donde el promedio en hombres es 49% superior a la de las mujeres.

Distribución de la densidad por rango de edad, Accidentes Personales



Fuente: CNSF

La ciberamenaza global. Tim Maurer y Arthur Nelson*

Las amenazas cibernéticas al sistema financiero son cada vez más frecuentes y la comunidad internacional debe cooperar para su protección.

Marco de referencia

El análisis del tema de “la ciberamenaza global” se basa en el artículo escrito por Tim Maurer y Arthur Nelson en la Revista Finance & Development, de marzo del 2021 en el cual los autores abordan un tema al que probablemente no se le ha dado la importancia que merece pero que recientemente se ha constituido como una enorme amenaza que afecta al sector financiero de los países y al sistema financiero internacional

Los autores inician su estudio haciendo referencia al hecho de que en febrero de 2016, unos hackers informáticos atacaron el banco central de Bangladesh y aprovecharon las vulnerabilidades de SWIFT, el principal sistema de mensajería de pagos electrónicos del sistema financiero mundial, para intentar robar 1,000 millones de dólares. Aunque la mayoría de las transacciones fraudulentas pudieron bloquearse, si desaparecieron 101 millones de dólares. El atraco fue una llamada de atención para el mundo de las finanzas de que los riesgos cibernéticos sistémicos en el sector financiero habían sido gravemente subestimados.

Hoy en día, la confirmación de que un ciberataque supone una amenaza para la estabilidad financiera es clara y evidente: no es una cuestión de si habrá un ataque o no, sino cuándo. Sin embargo, los gobiernos y las empresas del mundo siguen luchando para contener la amenaza porque sigue sin tener claridad sobre quién o quiénes son los responsables de proteger el sistema, y cada vez hay más las voces de preocupación y alarma. Al respecto, en febrero de 2020, Christine Lagarde, presidenta del Banco Central Europeo y exdirectora gerente del Fondo Monetario Internacional, advirtió que un ciberataque podría desencadenar una grave crisis financiera. En abril de 2020, el Consejo de Estabilidad Financiera (Financial Stability Board) advirtió que, si "un incidente cibernético no se llegara a contener satisfactoriamente, podría perturbar gravemente los sistemas financieros, incluidas las infraestructuras financieras críticas, lo que tendría muy graves y ampliamente diseminadas consecuencias para la estabilidad financiera". El potencial costo económico de este tipo de sucesos pueden ser inmenso y el daño a la confianza del público, muy significativo.

Actualmente, subsisten dos tendencias que agravan este riesgo. En primer lugar, el sistema financiero mundial está experimentando una transformación digital sin precedentes, que se aceleró con la pandemia de COVID-19. En este contexto, el resultado es que los bancos compiten con las empresas tecnológicas y las empresas tecnológicas compiten con los bancos. Mientras tanto, la pandemia ha aumentado la demanda de servicios financieros en línea y ha convertido en norma el trabajo desde casa. Al mismo tiempo, los bancos centrales de todo el mundo se están planteando la conveniencia de apoyar a las monedas digitales y modernizar los sistemas de pago y precisamente en esta época de transformación, en la que un incidente podría socavar fácilmente la confianza y hacer descarrilar estas innovaciones, la ciberseguridad es más importante que nunca.

En segundo lugar, los grupos maliciosos están aprovechando esta ola de transformación digital y se han convertido en una amenaza creciente para el sistema financiero mundial, para la estabilidad financiera y para la confianza en la integridad del sistema. La pandemia ha generado, incluso, nuevos objetivos a los hackers. Según el Banco de Pagos Internacionales (BIS por sus siglas en inglés), el sector financiero es el segundo más afectado por los ciberataques relacionados con el COVID-19, sólo por detrás del sector salud.

¿Quién está detrás de las amenazas?

Se espera que en el futuro se produzcan más ataques de este tipo con las consiguientes y graves afectaciones. Lo más preocupante son los incidentes que corrompen la integridad de los datos financieros, como los registros, los algoritmos y las transacciones. Actualmente se dispone de pocas soluciones técnicas para este tipo de ataques, los cuales tienen el potencial de socavar la confianza en general. Entre los actores maliciosos que están detrás de estos ataques se encuentran no sólo delincuentes cada vez más atrevidos -como el grupo Carbanak, que atacó a instituciones financieras para robar más de mil millones de dólares entre 2013 y 2018-, sino también estados y atacantes patrocinados por el Estado (ver Tabla1). Se estima que Corea del Norte, por ejemplo, ha robado unos 2,000 millones de dólares de por lo menos 38 países en los últimos cinco años.

Sin duda se trata de un problema mundial. Mientras que los ciberataques en los países de mayores ingresos suelen ocupar los titulares, se presta menos atención mediática al creciente número de ataques contra objetivos más vulnerables en los países de medianos y bajos ingresos. Sin embargo, es en estos países donde el impulso para lograr una mayor inclusión financiera ha sido más pronunciado, lo que ha llevado a muchas personas a dar el salto a los servicios financieros digitales, como los sistemas de pago por teléfono móvil. Aunque, indudablemente, se logran importantes avances en la inclusión financiera, los servicios financieros digitales también ofrecen un entorno rico en objetivos para los piratas informáticos. Por ejemplo, el hackeo realizado en octubre del 2020 a las mayores redes de dinero móvil de Uganda, MTN y Airtel, provocó una grave interrupción de 4 días de las transacciones del servicio.

Tabla 1.

Análisis de los ciberataques. Los responsables de estos incidentes no sólo incluyen amenazas de criminales sino también de estados y de grupos apatrocinados por los estados, con diversas metas y motivaciones			
ACTORES DE LAS AMENZAS	MOTIVACIONES	METAS	EJEMPLOS
Estados nacionales; grupos patrocinados por los estados	Geopolítico, ideológico	Disrrupción, destrucción, daño, amenaza, espionaje, ingresos	Corrupción permanente de datos, daños físicos dirigidos, disrrupción de redes de energía eléctrica, disrrupción del sistema de pagos, transferencias fraudulentas, espionaje
Cibercriminales	Enriquecimiento	Robo/ingresos	Robo de efectivo, transferencias fraudulentas, espionaje
Grupos terroristas, hackeractivistas, amenazas internas, inflitración	Diferencias ideológicas	Disrupción	Filtraciones, difamación, ataques para afectar los servicios

Fuente: Consejo Europeo de Riesgo Sistémico

La brecha de responsabilidad

A pesar de que el sistema financiero mundial depende cada vez más de la infraestructura digital, no está claro quién es el responsable de proteger el sistema contra los ciberataques. En parte, esto se debe a que el entorno está cambiando con rapidez. Lo grave es que si no se toman medidas concretas, el sistema financiero mundial se volverá más vulnerable a medida que la innovación, la competencia y la pandemia impulsen aún más la revolución digital. Si bien la mayoría de las amenazas se centran en obtener dinero, el número de ataques puramente perturbadores y destructivos ha ido aumentando; además, quienes aprenden a robar también aprenden sobre las redes y operaciones del sistema financiero, lo que les permite lanzar ataques más destructivos (o vender esos conocimientos y habilidades a otros). Esta rápida evolución del amplio mosaico de riesgos está poniendo a prueba la capacidad de respuesta de un sistema que, no obstante, es maduro y está bien regulado.

Por eso se dice que la mejor protección del sistema financiero mundial es sobre todo un reto organizativo. Los esfuerzos para reforzar las defensas y endurecer la normativa son fundamentales, pero no son suficientes para mitigar los crecientes riesgos. A diferencia de muchos sectores, la mayor parte de la comunidad de servicios financieros no carece de recursos ni de capacidad para aplicar soluciones técnicas. La principal cuestión se traduce en un problema de acción colectiva: ¿cómo organizar estratégicamente la protección del sistema entre los gobiernos, las autoridades financieras y la industria, así como en la forma de aprovechar estos recursos de forma eficaz y eficiente?.

La actual fragmentación entre las partes interesadas y las iniciativas se debe, en su mayoría, a los aspectos únicos y a la naturaleza cambiante del ciberriesgo. Las diferentes comunidades operan en sus propias trincheras y abordan el problema a través de sus respectivos mandatos. La comunidad de supervisores financieros se centra en la capacidad de recuperación, los diplomáticos en las normas de comportamiento del Estado, las agencias de seguridad nacional en tratar de disuadir la actividad maliciosa y los ejecutivos de la industria en los riesgos específicos de la empresa más que del sector. A medida que las fronteras entre las empresas de servicios financieros y las empresas tecnológicas se vuelven más difusas, las líneas de responsabilidad en materia de seguridad también se vuelven más vagas.

La desconexión que existe entre las comunidad financiera, la comunidad de seguridad nacional y la comunidad diplomática está particularmente acentuada. Las autoridades financieras se enfrentan a riesgos únicos derivados de las ciberamenazas, pero sus relaciones con los organismos de seguridad nacional, cuya participación es necesaria para hacer frente a esas amenazas de forma eficaz, siguen siendo limitadas. Este vacío de responsabilidad y la continua incertidumbre sobre las funciones y los mandatos para proteger el sistema financiero mundial alimentan los riesgos. Parte de la incertidumbre se debe al actual clima geopolítico y a los altos niveles de desconfianza, que dificultan la colaboración entre la comunidad internacional. La cooperación en materia de ciberseguridad se ha visto obstaculizada, fragmentada y, frecuentemente, limitada a los círculos de confianza más reducidos porque afecta en aspectos sensibles de la seguridad nacional. La cooperación internacional y entre múltiples partes interesadas no es un "nice-to-have" (deseable tenerlo) sino un "need-to-have" (necesario tenerlo).

Una estrategia internacional

Para lograr una protección más eficaz del sistema financiero internacional contra las ciberamenazas, la Fundación Carnegie para la Paz Internacional publicó en noviembre de 2020

un informe titulado "Estrategia internacional para la mejor protección del sistema financiero mundial contra las ciberamenazas". El informe fue elaborado en colaboración con el Foro Económico Mundial, por medio del cual se recomiendan acciones específicas para reducir la fragmentación, fomentando una mayor colaboración, tanto a nivel internacional como entre organismos gubernamentales, empresas financieras y compañías tecnológicas. La estrategia recomendada se basa en 4 principios:

- En primer lugar, se requiere una mayor claridad sobre las funciones y responsabilidades de los involucrados. En este sentido, se destaca que sólo unos pocos países han establecido relaciones internas eficaces entre sus autoridades financieras, las fuerzas de seguridad, los diplomáticos, otros actores gubernamentales relevantes y la industria. La fragmentación existente obstaculiza la cooperación internacional y debilita la capacidad colectiva de resistencia, recuperación y respuesta del sistema internacional en contra de los ciberataques.
- En segundo lugar, la colaboración internacional es necesaria y urgente. Dada la magnitud de la amenaza y la interdependencia global del sistema, los gobiernos, las empresas financieras y las compañías tecnológicas no pueden protegerse eficazmente contra las ciberamenazas si trabajan de forma aislada.
- En tercer lugar, al reducir la fragmentación de esfuerzos se liberará capacidad para abordar el problema de manera conjunta. Hay muchas iniciativas en marcha para proteger de mejor manera a las instituciones financieras, pero siguen estando aisladas. Algunos de estos esfuerzos se duplican entre sí, aumentando los costos de transacción. Varias de estas iniciativas están lo suficientemente maduras como para ser compartidas, mejor coordinadas y más difundidas internacionalemente.
- En cuarto lugar, la protección del sistema financiero internacional puede ser un modelo para otros sectores. El sistema financiero es una de las pocas áreas en las que los países tienen un claro interés compartido en la cooperación, incluso cuando las tensiones geopolíticas son elevadas. Centrarse en el sector financiero constituye un punto de partida y podría allanar el camino hacia una mejor protección en el futuro de otros sectores.

Entre las medidas para reforzar la resistencia cibernética, el informe la Fundación Carnegie recomienda que el Consejo de Estabilidad Financiera del G20 trabaje sobre un enfoque básico para supervisar la gestión de los riesgos cibernéticos en las instituciones financieras. Los gobiernos y el sector financiero deberían reforzar la seguridad compartiendo información sobre las amenazas y creando equipos de respuesta a emergencias informáticas financieras (CERT),

siguiendo el modelo del FinCERT de Israel, que es es el primer organismo certificador de educadores y asesores financieros, que promueve la eficiente provisión de productos de consumos financieros, servicios y educación a través de una certificación profesional a los individuos que proporcionan estos servicios.

Las autoridades financieras también deberían dar prioridad a la crecciente resilencia del sector financiero frente a los ataques dirigidos a datos y algoritmos. Entre ellas debería considerarse la posibilidad de contar con una bóveda de datos segura y encriptada que permita a los miembros hacer una copia de seguridad de los datos de las cuentas de los clientes durante la noche y también deberían realizarse ensayos regulares de simulación de ciberataques para identificar los puntos vulnerables y desarrollar planes de acción.

Con la finanlidad de reforzar las normas internacionales, el informe recomienda que los gobiernos dejen claro cómo aplicarán el derecho internacional al ciberespacio y refuercen las normas para proteger la integridad del sistema financiero. Los gobiernos de Australia, los Países Bajos y el Reino Unido ya han dado un primer paso con declaraciones en las que indican que los ciberataques desde el extranjero pueden ser considerados como un uso ilegal de la fuerza o intervención en los asuntos internos de otro Estado.

En este contexto, la resiliencia cibernética y el fortalecimiento de las normas internacionales pueden facilitar la respuesta colectiva a través de acciones de aplicación de la ley o de la reacción multilateral con la industria. Las respuestas pueden incluir sanciones, detenciones y confiscación de activos. Asimismo, los gobiernos pueden apoyar estos esfuerzos estableciendo entidades que ayuden a la evaluación de las amenazas y a coordinar las respuestas. La recopilación de información debería enfocarse sobre las amenazas al sistema financiero y los gobiernos deberían compartir dicha información con aliados y países afines.

Reflexiones sobre el desarrollo de la capacidad para hacer frente a los ciberataques

La estrategia global delineada en el informe de la Fundación Carnegie depende, a su vez, de identificar y reclutar al personal idóneo, especializado en ciberseguridad, así como de su capacitación, el fortalecimiento y la expansión de la capacidad de ciberseguridad del sector financiero y de la salvaguarda de los avances que se han logrado en materia de inclusión financiera asociados a la transformación digital.

El alto desempleo debido a la crisis sanitaria derivada de la pandemia del COVID-19 abre un campo de oportunidad para la formación y contratación de personas con talento para reforzar a

los grupos de expertos en ciberseguridad a nivel mundial. Las empresas de servicios financieros deberían invertir en iniciativas para desarrollar la cantera de talentos, incluyendo programas de educación vocacional, secundaria, capacitación en el trabajo y a nivel universitario en un contexto de transformación digital acelerada.

La construcción y/o reforzamiento de la capacidad en materia de ciberseguridad significa concentrar esfuerzos en prestar asistencia en el lugar y momento requeridos. El FMI y otras organizaciones internacionales han recibido solicitudes de asistencia en materia de ciberseguridad por parte de los estados miembros, especialmente tras el incidente de Bangladesh de 2016. Los gobiernos y los bancos centrales del G20 bien podrían establecer un mecanismo internacional para la creación de capacidad de ciberseguridad para el sector financiero, con un organismo internacional como el FMI encargado de coordinar los esfuerzos. Asimismo, la Organización para la Cooperación y el Desarrollo Económicos y las instituciones financieras internacionales podría integrar, por ejemplo, paquetes de apoyo y otorgar asistencia a los países que lo requieran en materia de construcción, formación y certificación de capacidades de ciberseguridad.

Por último, para mantener y continuar con los avances a nivel mundial en materia de inclusión financiera es necesario reforzar las conexiones entre la inclusión financiera y la ciberseguridad. Esto es especialmente urgente en África, ya que muchos países del continente están experimentando una importante transformación de sus sectores financieros a medida que amplían la inclusión financiera y pasan a los servicios financieros digitales. Por lo tanto, parece urgente y necesario crear una red de expertos centrada específicamente en la ciberseguridad en dicho continente.

Al parecer, ha llegado el momento de que la comunidad internacional -incluidos los gobiernos, los bancos centrales, los organismos supervisores, la industria y otras partes interesadas- se reúna y aglutine esfuerzos para hacer frente a este urgente e importante desafío. Una estrategia bien estructurada, que tenga como base las ideas mencionadas anteriormente, puede ser el punto de partida para integrar un plan que convierta dichas ideas en acciones. @

Fuente: Finance & Development. Marzo del 2021

* **TIM MAURER** es el director de la Inciativa de Cyber Policy y profesor emérito del Carnegie Institute del Programa de Tecnología y Asuntos Internacionales de Paz Internacional y **ARTHUR NELSON** analista investigador en la Iniciativa de Cyber Policy del Carnegie Institute.