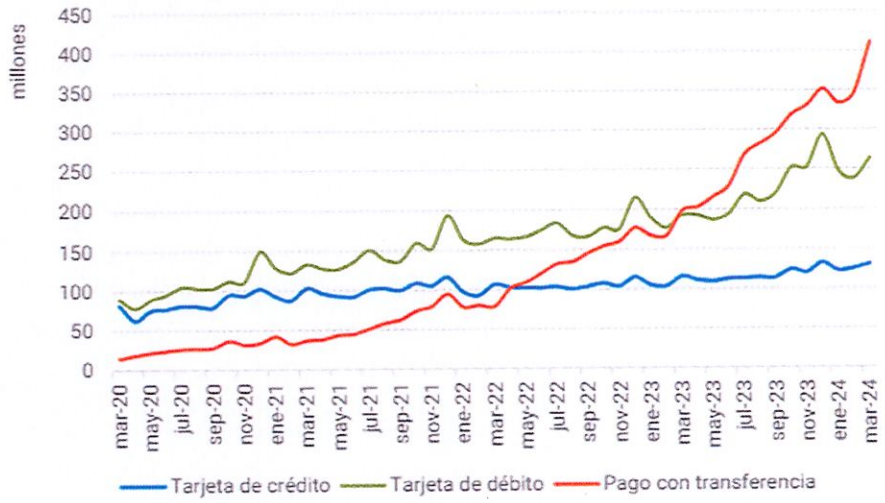
ANEXO 1 (Tecnología)

Los volúmenes y montos transaccionados por adulto en 2023 superaron a las transferencias electrónicas totales y se consolidaron como instrumento electrónico más utilizado para realizar pagos por segundo año consecutivo, cada adulto realizó en promedio 30 pagos electrónicos por mes, un 68% más que durante 2022. Los pagos inmediatos (transferencias y pagos con Transferencias PCT), fueron los que impulsaron el crecimiento y representaron 6 de cada 10 pagos, su uso implica mayores beneficios para los comercios en términos en plazos de acreditación y comisiones. En cuanto a los montos el 60% de ellos fueron operados a través de estos instrumentos. La cantidad de transferencias entre cuentas bancarias y cuentas de pagos por adulto creció por encima del 155% interanual. Los pagos con transferencias por individuos, en promedio desplazaron a las tarjetas de débito (24% vs, 20%) respectivamente del total de transacciones. El crecimiento interanual de los PCT (Pagos con transferencia) fue de un 103% en su mayoría impulsados por usuarios de un mismo PSP. Cabe destacar que dentro de los PCT interoperables, aquellos iniciados en un código QR motorizaron el crecimiento con una tasa de variación superior al total debido a la caída en los canales de POS y botón de pago.[17]

Gráfico 2. Operaciones con tarjeta de crédito[14], tarjeta de débito[15] y PCT[16] (cantidad)



[17] https://www.bcra.gob.ar/Pdfs/PublicacionesEstadisticas/informe-mensual-de-pagos-minoristas-abr-2024.pdf

Pagos con transferencia

Gráfico 10. PCT interoperable por método de iniciación (cantidad)

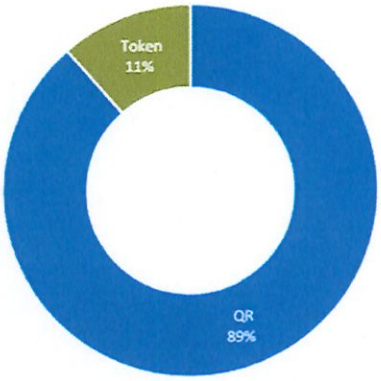
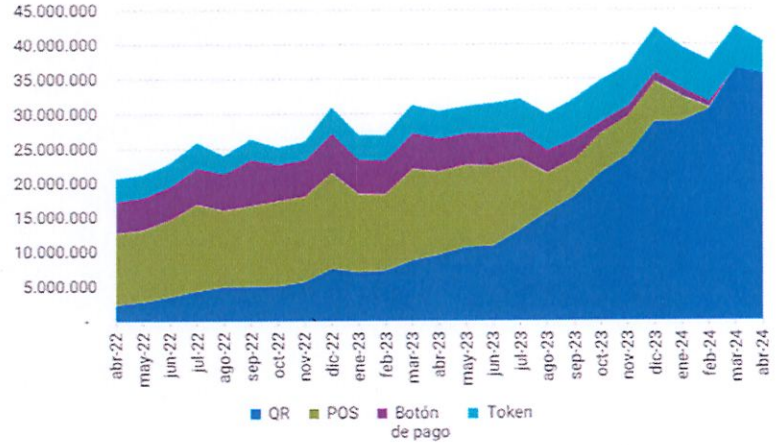
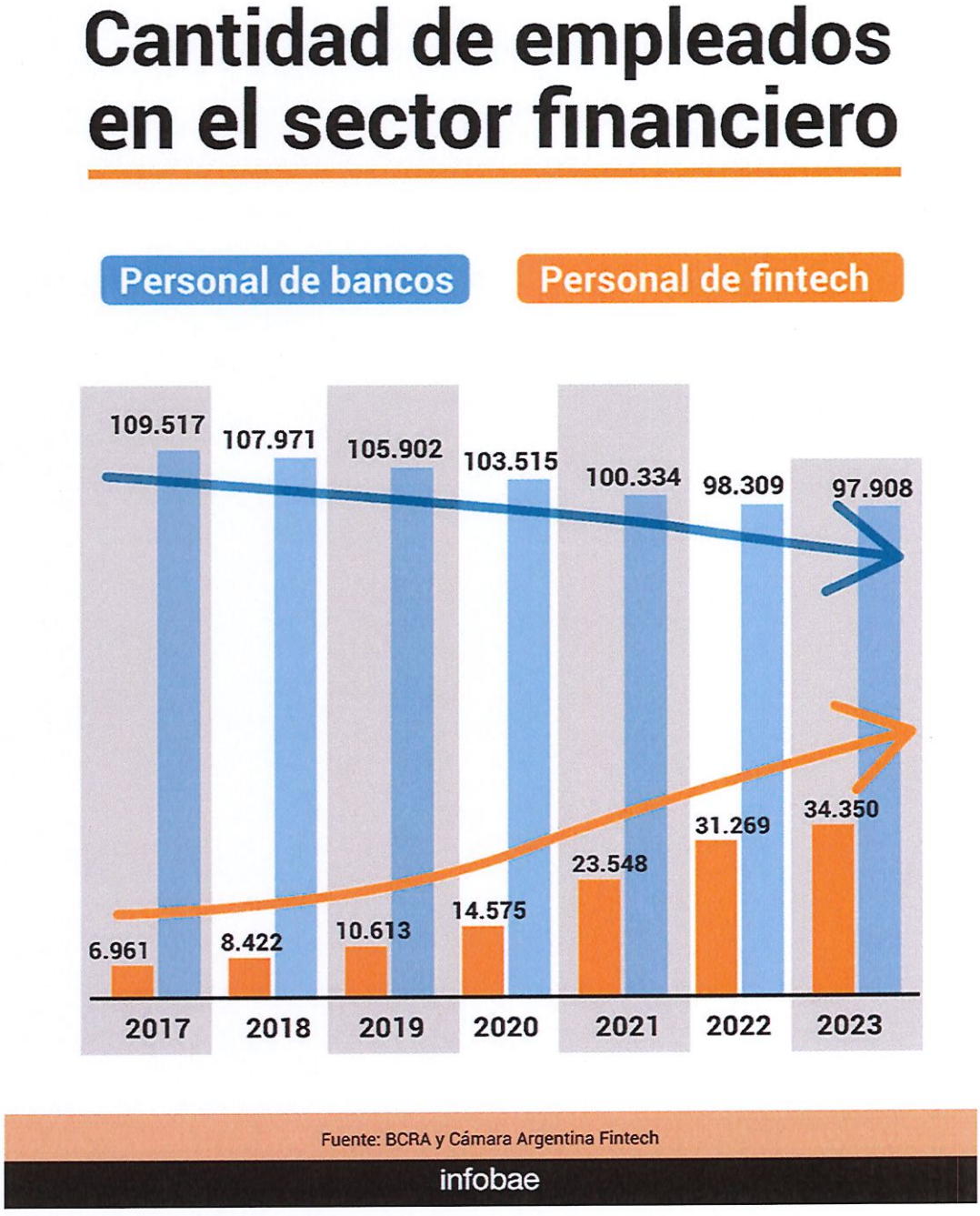


Gráfico 11. PCT interoperable por método de iniciación (cantidad)





La utilización de la inteligencia **artificial (IA)** ha tenido un impacto significativo en el sistema financiero tanto a nivel mundial como en Argentina y muestra de esto es que ya se utilizan algunos de estos programas, a mero título ejemplificativo (**Scoring Crediticio, scoring móvil alternativo** (permite que se pueda tener una calificación crediticia en minutos desde los celulares, incluso sino tienen historial crediticio bancario). Esta tecnología es reconocida y obtuvo el premio de la quinta edición **del Laboratorio CAF(Banco de desarrollo de América Latina de Inclusión Financiera)** y ha sido respaldada en su desarrollo por un financiamiento de hasta US$ 500.000 del BID.

Según *Diego Varela, CEO y cofundador de Findo, más* de 200,000 personas ya han experimentado acceder a servicios financieros a través de este sistema, y se espera llegar a otras 100,000 personas en 2024.[18] **Como informamos en despachos anteriores las instituciones financieras utilizan algoritmos de IA para analizar grandes cantidades de datos y predecir tendencias.** Estos avances y la expansión de los canales digitales en desmedro de la atención en las sucursales bancarias cambiaron el mapa del empleo financiero, con el impulso de la pandemia pero también de nuevas generaciones que ya no quiere hacer trámites presenciales de ninguna clase. La adopción de a IA requiere una colaboración estrecha y responsable entre el sector privado, los reguladores (BCRA) y las instituciones financieras pero lamentablemente si bien hay avances significativos quedan desafíos por superar como son la ética, la privacidad de los datos y la transparencia estos son aspectos críticos que deben abordarse para garantizar un uso responsable de la IA en el ámbito financiero **Esta comisión hace años que viene reclamando al BCRA mayores controles y regulaciones para las Fintech y sus cuentas y de la misma manera procedieron las entidades que agrupan a los bancos privados desde el año 2021[19] (ABA y ADEBA). El BCRA también es responsable de la política monetaria. A través de sus decisiones sobre tasas de interés y liquidez, influye en la economía y el sistema financiero. La regulación y supervisión del BCRA. de las normativas y reglas para las instituciones financieras, incluidos bancos y Fintech deben garantizar la estabilidad y la integridad del sistema.**

ANEXO 2 (DESREGULACIÓN)

Competencia desigual de Mercado Pago en la Argentina. La competencia desigual entre los bancos argentinos y Mercado Pago se ha convertido en un tema importante en el sector financiero. La cámara (ADEBA) expresó su preocupación por las regulaciones que rigen en el mercado de los medios de pago y argumentan que, en comparación con Mercado Pago, no operan en igualdad de condiciones en términos de servicios y regulaciones. El presidente de la cámara se refirió en el Centro de Innovación Financiera del Grupo Petersen, en Puerto Madero, **Javier Bolzico**, criticó las regulaciones vigentes y planteó que **"a iguales servicios, iguales condiciones"**, en clara referencia a la fintech de Galperin, Mercado Pago[20].

Denuncia por Abuso de Posición Dominante:
Los bancos han denunciado a Mercado Pago ante la Comisión Nacional de Defensa de la Competencia (CNDC) por abuso de posición dominante. Dicha denuncia fue presentada por la empresa MODO, la billetera virtual que agrupa bancos que operan en nuestro País. En ella señala que Mercado Pago incumple con la normativa dictada por el Banco Central (BCRA) que estaba vigente desde el 30 de abril de 2024 y se resistía a abrir sus sistemas e impide que su código QR acepte pagos de tarjetas de créditos ingresadas en otras billeteras virtuales. Luego de varias semanas de disputas y denuncias el BCRA mediante la comunicación A 8032 estableció que todas las billeteras virtuales están obligadas a leer todos los códigos QR y en la comunicación, el Central fijó la comisión máxima de 0,07 por ciento por operación que una billetera virtual, como Mercado Pago, puede cobrarle a un banco emisor por "intermediar" en un pago con tarjeta de crédito. Estableció que la presente comunicación entrará en vigencia de acuerdo con el siguiente cronograma: a. b. puntos 1, 2 y 3: 60 días contados desde la difusión de

[18] https://www.forbesargentina.com/columnistas/el-impacto-inteligencia-artificial-acceso-credito-inclusion-financiera-n50655
[19] https://www.cronista.com/infotechnology/finanzas-digitales/los-bancos-piden-nuevas-regulaciones-para-las-fintech-por-los-casos-de-estafas-que-esta-en-juego/
[20] https://www.a24.com/economia/billeteras-virtuales-los-bancos-vuelven-cruzar-al-dueno-mercado-libre-desventajas-la-competencia-n1325989

la presente comunicación; punto 4: 270 días contados desde la difusión de la presente comunicación."[21].

ANEXO 3 (Seguridad Bancaria)

Según la firma Kaspersky, se cuadruplicaron las estafas a través de los troyanos bancarios alcanzando los 10 mil ataques durante 2023: el equivalente de 30 atentados por día. Por ejemplo, el troyano Mekotio tiene un método original para sustraer información financiera y credenciales para el acceso a cuentas bancarias. Se moviliza a través de e mail y se enmascara en una notificación oficial de la policía federal engañando a las víctimas simulando que tienen una multa de tránsito y hay variantes donde alerta por una cuenta impaga. El accionar de este troyano consiste en recopilar datos a través de un registro de teclas, un capturador de pantalla o una superposición de la página de inicio de homebanking. Estas suplantaciones imitan a los bancos más populares de la Argentina. Lo grave de esta variante es que, una vez consumado el hurto, las entidades bancarias no responden reclamos argumentando que no son ellos los responsables de haber permitido el acceso al virus de la computadora. Los reportes de la firma ESET muestran que Argentina, con el 52 % es el país con más actividad de este troyano.

Esto parece sostenerse para lo que va del 2024 con la implementación de las últimas tecnologías, como la inteligencia artificial (IA) para elaborar un mayor volumen de explotaciones únicas y variantes nuevas de malware y ransomware, que son mucho mas dirigidos. Según Fortinet, argentina recibió más de 262 millones de intentos de ciberataques durante el primer trimestre del 2024 con cibercriminales que cada vez utilizan técnicas de reconocimiento y evasión más avanzadas y sofisticadas que aumentan sus probabilidades de éxito.

Las herramientas de Inteligencia Artificial emergentes facilitarán la producción de mensajes de *phishing* y la suplantación de identidad de personas específicas. Los atacantes pueden idear métodos creativos de automatización recopilando datos en línea y enviándolos a los Modelos de Lenguaje Grandes especializados para la IA, con el fin de elaborar borradores de cartas imitando el estilo personal de alguien cercano a la víctima.

El Equipo de Respuesta ante Emergencias Informáticas nacional (CERT.ar) de la Dirección Nacional de Ciberseguridad registró 379 incidentes de seguridad informática durante el año 2023 cifra que aumentó en un 13% respecto a la del 2022. Los casos de fraude, con 288 incidencias, representan el 76% del total de incidentes reportados, denotando que esta tipología fue el delito informático que más se registró durante el período mencionado. Entre los tipos detectados, se incluyeron uso no autorizado de los recursos, derechos de autor, suplantación de identidad y phishing.

Y a los efectos de la administración de incidentes, se consideraron doce sectores y haciendo un análisis anual, el sector más comprometido de acuerdo con los incidentes

[21] www.bcra.gob.ar/Pdfs/comytexord/A8032.pdf

reportados fue el de Finanzas con 117 casos, cifra que representa el 31% del total registrado.
Al realizar una discriminación por tipo de incidente informático, el phishing fue el más registrado con 286 casos, cifra que representa el 75,5% del total reportado estando la totalidad de casos del sector finanzas incluidos en este tipo de fraude.
En relación a un caso de phishing ocurrido en marzo del 2023, recientemente una entidad bancaria fue condenada y **si bien la damnificada era una persona jurídica, la magistrada consideró que debía aplicarse la Ley de Defensa del Consumidor y subrayo la falta de seguridad de la que adolecen las operaciones electrónicas**
Es así que en la demanda Quateck SRL c/ Banco Supervielle SA s/ daños y perjuicios incumplimiento contractual, la actora explicó que, mientras trataba de realizar una operación bancaria con su notebook, para lo cual debía acceder al homebanking cuyos datos se encontraban guardados en el dispositivo, al intentar realizar su operatoria, se le solicitaron claves enviadas a su mail y posteriormente posteriormente la página quedo bloqueada. Al comunicarse con el banco le informaron que no reportaban problemas en el sistema.
En ese momento le indicaron que era un **intento de fraude.** Horas después pudo constatar que la cuenta corriente de la empresa había quedado con un total de fondos transferidos de más de $8.000.000.-
Tras una respuesta negativa del banco al reclamo del cliente, aduciendo negligencia del empresario porque sus claves estaban en su notebook, se presentó la demanda además de penal, por daños y perjuicios. Es así que el perito informático determinó que **los montos no habituales de las transferencias, las características de las cuentas de destino y la reducida ventana de tiempo en la que se desarrollaron las operaciones hacían sospechar de que se trataban de transacciones fraudulentas**; las cuales no fueron advertidas por el sistema de seguridad informático del banco.
Incluso, calificó como inadecuados los controles de autentificación permitiendo que terceros accedieran al sistema informático suplantando la identidad física y digital de la parte actora. Puntualizó que era posible que hubiera dos ingresos simultáneos al homebanking y que el sistema de seguridad informático del banco no detectó el acceso no autorizado, por lo que no pudo bloquearlo por lo cual el banco **deberá responder porque su sistema de protección resultó insuficiente para prevenir e impedir las maniobras fraudulentas denunciadas**

La primera promueve el involucramiento del directorio y la alta gerencia en cuestiones que antes eran una preocupación exclusiva de las áreas técnicas. La resolución establece claramente la alineación con el negocio como punto de partida de todas las tareas y decisiones posteriores. El texto pone foco en el Gobierno de la Tecnología y Seguridad expresando responsabilidades muy claras para el Directorio, que ya no puede solo tomar conocimiento, sino que debe aprobar y supervisar las estructuras, los recursos, los marcos de gestión de riesgos y de continuidad del negocio. Y dentro de las novedades que trajo esta circular, se hace especial referencia a la necesidad de controlar y monitorear las terceras partes para gestionar los riesgos de ciberseguirdad.

En la sección 10.1 se establece que las entidades deben implementar una política y un marco sólido para la gestión de los procesos, servicios y/o actividades relacionadas a terceras partes con un mecanismo concreto de gestión. Dicho enfoque debe contemplar, entre otros aspectos fundamentales, las medidas de seguridad de acuerdo con los resultados de la gestión de riesgos de tecnología así como los riesgos vinculados a la delegación de dicha tarea considerando la definición de los roles y responsabilidades para las distintas actividades de gestión; procedimientos para la selección y contratación de terceras partes; la identificación de los puntos de contacto para los aspectos legales y los relacionados con la tecnología, seguridad de la información y gestión de ciberincidentes; la implementación de auditorías independientes sobre los servicios y actividades gestionados por terceras partes que permitan evaluar la gestión de riesgos y la alineación con los procesos de tecnología y seguridad de la información de la entidad.
Por otra parte, las entidades deberán evaluar posibles escenarios de finalización planificada o forzada de los procesos, servicios o actividades provistos por terceras partes, y establecer planes de finalización que les permitan mitigar los riesgos de interrupción, incumplimiento de los requisitos legales y regulatorios, o degradación de la calidad. Los planes de finalización deberán considerar la obtención de los datos, los programas fuentes, y la documentación de los sistemas y aplicaciones.
En la sección 10.3 se establece que las organizaciones deben definir un proceso de control que les permita realizar un seguimiento y evaluación de los procesos, servicios y actividades de tecnología y seguridad de la información delegados a terceras partes
La periodicidad de las actividades de control y monitoreo deberá definirse de acuerdo con el nivel de riesgo y lo critico de los procesos, servicios o actividades delegados.
En cuanto a la seguridad física de las trabajadoras, trabajadores bancarios y clientes sostenemos la necesidad de contar con personal de seguridad en las sucursales, contratados directamente por las entidades con convenio bancario así como también al personal de limpieza, ya que ambas tareas son tercerizadas precarizando a quienes las realizan.
Se continua con el monitoreo de seguridad a distancia, estando este sector también tercerizado y en muchos casos no contratados con convenio bancario. Esta metodología es utilizada en mayor medida para el control de las y los trabajadores más que para su seguridad. Funcionan como sistema de supervisión a distancia.