CIUDAD DE MÉXICO, 24 DE MAYO DE 2018.

VERSIÓN ESTENOGRÁFICA DE LA CONFERENCIA DE PRENSA OFRECIDA POR EL ING. MARCOS MARTÍNEZ GAVICA, PRESIDENTE DE LA ASOCIACIÓN DE BANCOS DE MÉXICO, EFECTUADA EN EL AUDITORIO DE LA PROPIA ABM.

- MARCOS MARTÍNEZ GAVICA: Muy buenas tardes. Muchas gracias por atender a nuestra conferencia de prensa después de la comida de asociados, con la invitación a las autoridades como lo hacemos regularmente.

Les tenemos una referencia de presentación, como siempre. Vamos a comenzar con ella.

Bueno, vamos a hablar, como siempre, del crédito, la captación, de la cartera vencida, etcétera.

El crédito, afortunadamente, sigue creciendo prácticamente a doble dígito, es una tendencia continuada desde hace muchos trimestres.

Habla también de un país que sigue creciendo económicamente, mejor de lo que todo el tiempo se ha estado esperando. Y como ven aquí, resalta el crecimiento de la cartera de crédito a las empresas que crece a más del 14 por ciento.

Pero también consumo y vivienda crecen a un porcentaje importante, de más del 8 por ciento y sólo son las carteras de gobierno y financieras las que no está creciendo. Pensamos que nuestra mezcla y el esfuerzo está muy bien, dado el crecimiento del país y los objetivos, y las principales necesidades, esto está muy bien.

Y en cuanto a la calidad de la cartera, podemos hablar de que seguimos creciendo a muy buen ritmo, pero lo seguimos haciendo con calidad, de esta manera en el que la cartera total su morosidad se mantiene estable en el 2.2, y donde las variaciones que pueden observar son mínimas y son las de antes.

Empresas, mejora que hace, la última vez que nos vimos estaba como pareja; consumo que estaba en 4.4, ahora en 4.5, o sea, prácticamente lo mismo y vivienda que tiene una décima porcentual más.

Entonces, con esto lo que les decimos es: sigue el crecimiento muy bien y con muy buena calidad de cartera.

Y hablando del otro lado, estas son las coberturas: seguimos de cualquier forma con una cobertura más que suficiente para la cartera vencida que tenemos en donde cubrimos más el consumo que las otras.

Vivienda es la única que está por debajo del 100 por ciento, y esto tiene una lógica, tenemos la garantía, y cuando tienes la garantía no hace falta constituir reservas del 100 por ciento porque la garantía cuenta y cuenta bien.

Entonces, buen crecimiento, buena calidad, bien reservada, como ven aquí.

Y hablando de la captación, la captación también sigue creciendo muy bien. Y otra vez, lo que es importante, las personas están prefiriendo invertir a plazo más que en mercado de dinero y dentro de la banca. La vista que tiene que ver la bancarización y la operatividad crece también a 9 por ciento, y este es un comportamiento que ha venido mostrando positivo ya por muchos meses.

Entonces, hablando de la operación bancaria, no traemos más láminas, porque creo que este es un buen resumen de decirles que la banca sigue creciendo bien, sigue creciendo muy bien en los sectores en donde hay más interés, sigue teniendo cartera de calidad, sigue muy bien provisionada y la captación que es la contraparte también sigue creciendo al mismo ritmo, con lo cual las mismas carteras de los clientes en ahorro son las que están financiando las carteras de crédito de nuestros clientes. No hay mejor equilibrio para una banca comercial.

En esta ocasión les traemos como tema, si ustedes recuerdan cada trimestre les traemos un tema especial las carteras hipotecarias consumo, en esta ocasión les traemos el Sistema de Pagos Interbancarios, que nos parece que es el tema que más interesa en este momento, por supuesto a ustedes, pero también en la sociedad en general.

Entonces, les vamos a dar un repaso con un breve antecedente de dónde sale el SPEI, cómo está y qué sucedió y qué esperamos que suceda.

Primero les diríamos que en los años 90 las transacciones financieras en México se habían vuelto más complejas y su monto había crecido muy significativamente, y en respuesta a esto, el Banco de México inició una reforma integral del Sistema de Pagos para hacerlo más seguro y más eficiente, y en 95 comenzó a operar un Sistema de Pagos Electrónico que le llamó de Uso Ampliado, el SPEUA.

En ese inicio, el Sistema sólo operaba con montos muy grandes, medio millón de pesos que en el 95 era una cantidad importante.

En el 96 evolucionó muy rápidamente y se bajó a 100 mil pesos, y un año después hasta 50 mil pesos.

Años después, en el 2004, se sustituyó o inició operaciones el Sistema de Pagos Electrónicos Interbancarios, el SPEI, que permitió desde entonces los pagos en tiempo real.

Los montos mínimos de operación en el SPEI fueron disminuyendo paulatinamente, y hoy en día se pueden realizar operaciones sin monto mínimo en el SPEI está abierto para cualquier transacción electrónica; e incluso se pueden operar desde los teléfonos móviles, e incluso --como pueden ver en la gráfica-- desde diciembre de año pasado en un esquema de 24 por 7; o sea, todo el tiempo pueden operar cualquier cliente, cualquier monto en términos reales.

Esto es realmente un avance tecnológico y de cambio de hábito importantísimo que nos mencionaba el Gobernador del Banco Central hace unos momentos, que este SPEI es el único en el mundo que opera con esa dimensión, que hay SPEI que operan, pero operan para operaciones interbancarias, nunca llegando un cliente y para montos grandes; y entre bancos y no personas.

Entonces, lo que tenemos en México es algo que no se tiene en el resto del mundo y como funciona es algo espectacular porque cabe cualquier tipo de operaciones, ya veremos magnitudes más adelantes.

Aquí está como el desarrollo de los sistemas ha permitido sustituir a los métodos de pago tradicionales por los electrónicos y especialmente estamos hablando del SPEI, en donde en los últimos 12 años han tomado gran relevancia estas metodologías de pagos electrónicos; el año pasado se realizaron 480 millones de pagos vía SPEI y su valor fue de 270 billones de pesos.

El desarrollo de medios de pago electrónicos ha permitido sustituir paulatinamente los medios de pago tradicionales, como es el caso de los cheques, y ahí lo ven claramente en la gráfica, es rojo es la operación de cheques y el azul son el total de las transferencias.

Mientras que los cheques disminuyeron un 55 por ciento su operatividad en los últimos 12 años, las transferencias electrónicas crecieron 232 por ciento, y las operaciones específicamente vía SPEI crecieron prácticamente 8 mil por ciento, 7 mil 900 por ciento.

Este crecimiento en los pagos electrónicos ha sido mucho mayor que el crecimiento que han tenido las operaciones en los cajeros, por ejemplo, que han crecido un 64 por ciento.

Y resulta muy lógico. Nuestros clientes ahorran tiempo y recursos al realizar sus pagos electrónicos a través de un portal bancario o desde su teléfono celular, en vez de emitir o cobrar un cheque, o bien, desplazarse a un cajero automático para retirar efectivo y, posteriormente realizar un pago.

Esto evidentemente, en el fondo, beneficia a nuestros clientes, pero también a nuestra economía y a la competitividad del país.

La seguridad es un factor imprescindible, y el esfuerzo en ella, el crecimiento que han registrado estos sistemas ha sido acompañado igualmente de esfuerzos muy grandes en materia de seguridad informática por parte de los bancos, que nos permite hacer frente a las contingencias y seguir garantizando la continuidad de la operación y de los servicios a nuestros clientes.

Y esto ha sido creciente. Cada vez hay más inversión de las bandas criminales que tratan de sacar provecho tecnológico, son los hackers, invierten mucho, están en esto todo el día, y la banca invierte mucho y se trata de defender de ellos.

Ese es un juego que ahí está. No acaba de empezar, lleva muchos años, nunca va a terminar, es de aquí en adelante.

Lo que aquí les mostramos es cómo en un breve sondeo entre los bancos, las primeras cifras que nos dan preliminares, y yo creo que son mayores, la banca invierte aproximadamente dos mil 400 millones de pesos anualmente en temas de seguridad informática, no digo en sistemas y no digo en infraestructura, únicamente en defenderse y tener sistemas con más fortaleza frente a ataques de estos hackers.

Estamos constantemente en contacto con otras organizaciones, estamos con los sistemas financieros, también en un intercambio de tecnología y de información, incluso por aquí creo que dice “pruebas de estrés y hackeo ético”.

Prácticamente todos los bancos tienen algunas pruebas de estrés, en donde ponen a sus sistemas bajo condiciones de ataque, para ver que lo resistan y prácticamente la mayor parte de los bancos, yo en un futuro no dudo que sea una obligación regulatoria, tenemos hackers éticos, que son hackers profesionales, pero de los buenos, los contratamos nosotros para que traten de infiltrar nuestros sistemas constantemente, y lo bueno es que cuando logran infiltrarlo, entonces encontramos dónde estamos vulnerables y los corregimos. Prácticamente lo hacen casi todos, y los bancos internacionales todos.

Y creo que podemos enseñar algo de los sistemas. Aquí lo que hay son unas fotos de los cuartos de mando, este es de algún mando, los monitores de su cuarto de mando de sus áreas de sistemas.

Algunas de las pantallas que ahí ven, en este caso creo que es la blanca que está en medio, está detectando en el tiempo real cuántos hackers están intentando entrar en el sistema, y les diría son muchas lucecitas y gráficas, que en el fondo lo que nos muestran es que hay más de mil intentos constantes en cada banco de hackers intentando entrar por nuestros sistemas; o sea, no es ninguna novedad y lo será mucho menos en el futuro. No es algo nuevo para el sistema, es algo tan antiguo como que ahí está previsto en el mero centro de los cuadros de mando de las operaciones.

Nos mantenemos también con mucho apego a la regulación local y a las mejores prácticas internacionales.

Dentro de la regulación de esta materia podemos señalar la Circular Única de Bancos de la Comisión Nacional Bancaria, que nos establece una normativa sobre banca electrónica y la operación y seguridad en la contratación de servicios de apoyo tecnológico.

Por su parte, el Banco Central establece las reglas de operación del SPEI.

Asimismo, los funcionarios bancarios que participan en estas operaciones en las diferentes áreas tecnológicas también tienen normatividad y pasan por la norma IT-ISO-9001, que atiende la gestión de calidad en Tecnologías de la Información con la norma ISO-27000, que asiste el desarrollo, implementación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información.

Estas son normas que nos pone la Comisión Nacional Bancaria, pero que están avaladas por la Organización Internacional para la Estandarización, el ISO, y la Comisión Electrónica Internacional, el IEC; también contamos con certificaciones internacionales bajo lineamientos acreditados por la ANSI, de American National Standards Institute.

En fin, como ven, es un tema de la mayor atención para la banca, lo ha sido y seguirá siendo en el futuro.

¿Qué pasó? ¿Qué es lo sucedió? Y esperemos que esta lámina, yo creo que todos ustedes lo tienen muy claro porque ya hemos hablado muchos de este tiempo de esto, pero dando un repaso:

Así fue la operatividad casi generalizada. En el ejemplo la institución A, en azul, lanza a través de SPEI recursos por 10 mil pesos hacia la institución B, que es la amarilla. Para conectarse al SPEI hay un programa, un software, que es el conecta al banco A con el SPEI. A través de ese software pasan los 10 mil pesos.

En algún tipo de software utilizado por algunos bancos, éste fue el que lograron hackear. ¿Y qué fue lo que hicieron? Que metieron operaciones adicionales.

Esa roja que ven ahí, es una operación que no salió del banco A, que la metió el hacker al conector, pero quiso que cuando el SPEI del banco A llegó al Banco Central, ya iba por 10 mil 001 pesos en lugar de por 10 mil pesos.

Acto siguiente el SPEI le mandó al banco B, el de amarillo, recursos por 10 mil 001 pesos. ¿Por qué puede mandarlos por 10 mil 001 pesos? Porque en el SPEI dentro del Banco Central cada banco tiene una cuenta y tiene fondos; entonces, tiene fondos sobrados. Entonces, de esos fondos tomaron demás de los 10 mil, el peso adicional.

Y cuando llegan al banco amarillo, al B, se entregan los 10 mil pesos que había mandado el banco A, con sus destinatarios los que eran normales, y por eso es que ningún cliente perdió dinero, sino lo que salió llegó, hablando del dinero de clientes, pero hubo un peso que lo metieron acá, que salió de la Tesorería del Banco, y que llegó a una cuenta que los hackers habían abierto en el banco B, a su nombre, entonces ese peso fue a una cuenta de una persona física, y esa persona, en cuanto llegó, retiró el dinero.

Evidentemente hay una conexión, es una persona, es una banda, unos señores que hackean, se meten al sistema, lo adulteran y le sacan más recursos. Y luego abren cuentas en otros bancos y hay gentes que van y retiran en efectivo el depósito que acaba de llegar.

Estos señores de acá, son cómplices. Estos señores son más identificables, estos son más difíciles de encontrar los que intervinieron el conector. Los otros existen y de los otros, en alguna medida hay más información. Y esos señores son personas, como les decimos, son personas físicas que se prestaron, a cambio de un porcentaje del depósito, a retirarlo, darles el dinero y quedarse con una parte.

¿El dinero cómo se va?, pues lo depositaron en otro lado, y ¿cómo se lo regresan?, no sabemos. Lo que sí sabemos es que, sobre estas personas, sí hay fotos de los bancos, sí hay registros y sobre ellos se está actuando, está actuando cada banco con sus distintos sistemas de seguridad y con la PGR.

Bueno, esta es la mecánica, es la que conocemos y es la que hemos tratado de combatir con las medidas que ya ustedes conocen.

Ahora, ¿qué es lo que nos tiene muy ocupados?

Como parte final de esta, o semifinal de esta presentación, quedan dos láminas para comentarlo con ustedes en preguntas y respuestas.

Como ven el monto comparado con la operatividad o la capital de la banca, el monto en promedio, dicen, los únicos que lo pueden saber en todo caso son las autoridades porque son los bancos con los únicos que están obligados a enseñársela es al Banco Central y a la Comisión Nacional Bancaria.

Aparentemente son 300 millones, puede que sea menos, porque algunas cuentas sí se cerraron.

Si comparamos 300 millones con el billón 100 mil de operación diaria en el SPEI, el porcentaje ni se los pongo porque es 0.00000 lo que sea.

Qué les diríamos, o contra el capital de la banca que son 974 mil millones, no hay impacto.

¿Dónde sí hay impacto? En que hay retrasos en la operación y esto le ha causado molestias a nuestra clientela que estaba acostumbrada a que ya la operación era en tiempo real, bueno, eso sí nos preocupa más; o que les dé miedo que qué pasó con su dinero.

Ahora ya sabemos que no les pasó nada, pero en un principio la gente tuvo algo de miedo por falta de información, algo o mucho, y alguna desconfianza de si el sistema financiero era seguro o no era seguro.

Hoy queda claro que el sistema financiero es seguro, que el SPEI es seguro, que ningún cliente perdió absolutamente nada y que ya está detectado dónde fue que pudieron infiltrarse y que estamos tomando medidas para que por lo menos en esta modalidad ya no suceda.

¿Qué estamos haciendo adicionalmente? El Comité de Ciberseguridad de la ABM que trabaja constantemente en este tema, ha sido reforzada y se ha puesto a trabajar en coordinación con las autoridades para desarrollar más medidas que nos aseguren que por lo menos esta modalidad queda bloqueada. Y esa es una prioridad del corto plazo.

Ya no encontramos eventos, no les podemos asegurar aquí que ya no va a haber eventos, pero de momento no hay.

Estamos viendo cómo reforzamos más, pero que al mismo tiempo regresemos a la operación normal para los clientes, o sea, la del tiempo real lo antes posible, y después ya hemos establecido distintos grupos de trabajo y mecánicas para reforzar los protocolos de seguridad entre los bancos, los protocolos de seguridad de colaboración con las autoridades.

De hecho, venimos en este momento de firmar un convenio entre la Secretaría de Hacienda, el Banco de México y la Comisión Nacional Bancaria, y las principales asociaciones financieras del país, estuvimos nosotros, fueron 10, fueron muchas, ustedes están recibiendo el comunicado de prensa en este momento.

¿Y cuál es la idea? Coordinarnos mejor, reforzar mejor, intercomunicarnos mejor y crear mejores protocolos de seguridad, en algo que sabemos que ni es nuevo ni se va a acabar, se va a acabar este más, muy probablemente ya se acabó, pero seguirá habiendo estos miles de intentos constantes en todos los bancos, en cada banco y en cada institución financiera no bancaria.

Y como es una actividad que existe en el mundo en la industria bancaria, pero también en el resto de las industrias, incluso gobiernos como ustedes que ya tienen algunas historias, pues entonces se trate de que no te ganen los malos, sino de hacer un trabajo que te proteja y te mantenga a salvo.

¿Qué es importantísimo para nosotros además de la atención al cliente y de la seguridad de que su dinero está a salvo? Pues el que no nos pase, el que no suframos problemas de atención a nuestra clientela.

Pero ese mensaje sí es clarísimo: ningún cliente sufrió ningún quebranto económico, y si hay alguno o algunos que tienen algún cargo, porque ellos sí pagaron su crédito hipotecario, pero no llegó porque la transferencia tardó tiempo en llegar, no tendrán problema, enseñando la documentación todos los bancos del sistema estamos más que dispuesto a que sabiendo que no fue su culpa no van a tener ninguna penalidad, lo aseveremos los bancos.

Y que esos 300 millones o lo que sea, fue de recursos de los bancos, y que es una cantidad que afecta ni al patrimonio ni a la solvencia de ninguna de las instituciones.

Pues con esto me pasaría a la última, en la creo que ya se las dije, entonces ya no se las repito, porque es lo que les acababa de decir.

Bueno, con esto estamos a sus órdenes para que comentemos este tema, que entre esto y lo político se han vuelto los dos temas de todo el día para nosotros. Y hoy éste. Ese lo vamos a dejar para otro día.

A sus órdenes.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Iniciamos con la sesión de preguntas y respuestas con la intervención de Toño Hernández, del El Universal.

- ANTONIO HERNÁNDEZ: Buenas tardes. Creo que vas a tener muchas preguntas, Marcos.

Quiero preguntarte primero. Desde finales del año pasado ya habían ocurrido frades similares en cantidades muy pequeñas, BANCOMEXT incluso también fue un esquema ya venía alertando, por decirlo así, de un gran golpe; los bancos no se prepararon ante algo que parecía inminente. Esa es la primera pregunta.

¿Los 300 millones de pesos ya es, ya se asume como pérdida, es factible que se recupere algo? Comentabas que al principio hubo miedo por parte de los clientes porque no pasaban los SPEI. Preguntarte: temen un efecto reputacional en la operación de los clientes antes efecto que tuvimos.

Entre las líneas de investigación que hay, se maneja que hay tanto empleados de los proveedores, de los bancos e inclusive, de las mismas autoridades que podrían estar infiltradas. ¿Qué información tienen sobre esto?

Y, por último, qué va a pasar con los proveedores que fallaron. ¿Ya no van a ser autorizados para operar con los bancos, se les va a pedir una regulación más fuerte? Son esas Marcos. Gracias.

- MARCOS MARTÍNEZ GAVICA: Al contrario, gracias a ti.

Bueno, como les hemos comentado. No es de fines del año pasado. Desde hace años hay intentos de hackeo constante, múltiples y desde hace años hay hackeos exitosos en algún banco, en alguna operación.

El caso es que son hackeos que se entera el banco y lo resuelve.

Entonces no está conectado. No es un solo evento que se tenga continuidad, son muchísimos, y, de hecho, nosotros no tenemos esa información, pero lo que hemos escuchado de las partes oficiales es que es el caso, hablando de banca, de tres bancos en cuyo caso, por esa razón la ABM tampoco ha salido desde un principio a hablar de este tema porque no es un problema del sistema, es un problema de tres bancos. Y, es más, es un problema de ese software que utilizan esos tres bancos.

En cuyo caso se volvió grande el tema, porque se manifestó en clientes y en un retraso en el tiempo de entrega. ¿Por qué fue el retraso?, porque una vez que fueron alertadas las autoridades y tuvieron conocimiento de que eso estaba sucediendo, pues entonces sí pasas la comunicación y los bancos deciden tomar protocolos de otro tipo de seguridad, pero con características distintas.

¿Qué significa distintas? El sistema alterno que tarda más tiempo. Y ahí, pues todos ustedes y los clientes comenzaron a verse extrañados por qué ahora no era en tiempo real, pero por eso fue del conocimiento algo que es de tres bancos.

Por eso 300 millones, nosotros no sabemos. Las cifras exactas en este momento de cuánto es, la tiene cada uno de los bancos que tuvieron ese problema y las autoridades a las que se lo reportan, pero a la Asociación de Bancos, evidentemente no nos la pasan, entonces no sabemos.

El tema reputacional. Por supuesto que es el que nos preocupa, por eso se los estamos poniendo como lo que más nos preocupa, pero por eso les estamos diciendo la banca es segura y su dinero ha estado y seguirá seguro.

Y ahí sí, esta Asociación está clarísima de que eso es así, y no sólo por el *feedback* que nos dan los bancos, sino porque ya sabemos que el quebranto fue a las tesorerías de los bancos y no a ningún cliente, y porque cualquier cliente que se vea afectado está el compromiso de la banca de que se hará cargo de esa afectación.

Si hay gente dentro de fuera la ABM no lo sabe, eso es parte de la investigación que cada uno de los bancos afectados está haciendo, bueno, le llaman algo muy raro, algo de muertos, que es el forense, ojalá y esto sea forense, o sea, que sí ya esté muerto; si ya se murió pues qué bueno y ya sabrán ellos, y el proveedor, pues el proveedor que para su desgracia le encontró vulnerabilidad porque igual hizo un trabajo muy profesional pues su sistema tiene que corregirlo.

No sé si mis colegas quieren decir algo.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: La siguiente pregunta corresponde a Edgar Juárez.

- EDGAR JUÁREZ: Hola, buenas tardes.

Comentas, Marcos, que fue un problema de tres bancos en específico que tenían este proveedor. No sé si a su consideración o qué les haya dicho el Gobernador del Banco de México, el Banco de México en su conferencia la semana pasada que fue porque no habían cumplido, o no habían cumplido hasta ese momento con lo que marcaba la circular de hace aproximadamente un año.

Entonces, sí es necesario que estos bancos sean castigados, bueno, no sé si la autoridad vaya a sancionarlos, pero desde su parte como gremio estos tres bancos no afectan la imagen de todo el gremio y, por lo tanto, tendrían que ser sancionados.

Si me pudieran regalar un poquito su opinión, porque nos comentaste ya un poco de qué trató la firma de las bases, que firmaron hace un momento, pero cuál es su opinión y si a partir de cuándo estarán integrados estos grupos, tanto de la autoridad, como de los bancos para, estos grupos de reacción que le llaman, me parece.

Y si entiendo entonces hasta la fecha los bancos no tenían estos grupos de reacción inmediata ante cualquier incidencia o estaban catalogados en otra área.

Y entonces nada más para dejarlo claro, este problema, este hackeo ya lo podemos dar por terminado, ya quedó ahí, ya no va a haber ningún otro

intento, no queda vulnerable el sistema ante este hackeo y si pudiera ser más vulnerable todavía precisamente por lo que ocurrió.

Gracias.

- MARCOS MARTÍNEZ GAVICA: A ver, déjame empiezo al revés, para acordarme. Luego me vas recordando.

Como les decimos, no podemos asegurar que está muerto, ojalá y el muerto esté muerto y por eso sea forense. Parece que está muerto. Es porque ya se detectó esa vulnerabilidad, entonces esa puerta está cerrada.

Hablando de cuándo comienza a actuar, como les decimos, dentro de cada banco el área de ciberseguridad es un área importantísima a la que se le dedican una cantidad de recursos muy fuertes, como vieron ahí, era una primera visión 2 mil 400 millones de pesos por año; entonces, tampoco es algo nuevo.

El Comité de Ciberseguridad de la ABM tampoco es nuevo, debe de llevar, trabajando en esto, septiembre del año pasado. Pero los bancos muchísimo tiempo.

¿Cuánto tiempo llevamos trabajando en esto? Desde que nos dieron a conocer que había un problema. Y el grupo ya en combinación con las autoridades desde principios de mayo que fue cuando se conoció un poco más de este tema.

Lo que firmamos ahora con las otras asociaciones e intermediarios es un convenio en el que nos comprometemos a compartir más información y a trabajar más en conjunto, porque, como les decíamos, estos temas no nada más le pasan a la banca, sino a muchas empresas y a muchos tipos de actividades.

Entonces, eso de hoy son convenios de colaboración y de obligación de compartimiento de información.

- EDGAR JUÁREZ: Eran un poco más en el sentido de que si este caso no deja al Sistema Financiero Mexicano todavía más vulnerable al que intenten hackearlo desde otros puntos, que sea un punto más.

- MARCOS MARTÍNEZ GAVICA: Pues, mira, fuera de los miles que hay en cada momento, éste en el que fuimos vulnerables está cerrado; entonces en este momento no estamos vulnerables.

Hace tres semanas tres bancos no hay sistema, tres bancos fueron vulnerables a un hackeo.

- EDGAR JUÁREZ: Y la otra era respecto a lo que comentaba Banco de México de que hay algunos bancos que no había cumplido esta circular. Si merecen algún tipo de restricción o llamado de atención del parte del gremio por afectar así al sistema.

- MARCOS MARTÍNEZ GAVICA: Pues, mira, como nosotros no somos sus jefes, qué te puedo decir. Pero la autoridad sí estará hablando con los que ellos piensen que no ha cumplido, que a lo mejor son otros, a lo mejor estos cumplieron; puede haber cumplido, la vulnerabilidad no tiene que ver con si hiciste el trabajo o no, o que si tu banco es bueno o no, porque aunque no tenemos nosotros los nombres de los bancos, lo que sí les puedo decir es que pudo haber sido el mejor banco en sistemas, uno de los hackeados, nada más tenía esa debilidad, con sistemas buenisisísimos, mejores que el promedio de los bancos. Esto no es porque encontraron un banco con muy malos sistemas, encontraron ese punto.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Gracias. Jessika Becerra de Reforma. Por favor, Jessika.

- JESSIKA BECERRA: Buenas tardes. Yo quiero conocer su opinión sobre la opinión del Banco de México. Lo dijo el día de la conferencia, lo dice hoy en un documento que “es responsabilidad de los bancos”, prácticamente les está echando la culpa a ustedes, que fueron sus proveedores, que fueron sus conexiones, que fueron sus cuidados.

Entonces, yo quisiera saber qué opinan de que Banco de México prácticamente se quede sin responsabilidad y les eche la culpa a ustedes,

Cuántos bancos no han cumplido esta normatividad que viene desde el 2017, que debieron ya incorporar en enero. El Banco también dice que no cumplieron estas disposiciones, algunos. Yo quisiera saber cuántos son los bancos que la cumplieron.

Y respecto a los 300 millones de pesos, quisiera dejar claro de una vez si fueron transferencias o fueron retirados completamente estos 300 millones de pesos, y ¿cómo los cobran los bancos? Entiendo que tienen ustedes seguros, el BBB, el seguro cibernético, cómo es que quedan cubiertos con capital para esto o entra el seguro. Y si me pueden aclarar eso, ¿fueron transferencias y sólo una parte se sustrajo? O se sustrajo todo. Gracias.

- MARCOS MARTÍNEZ GAVICA: Gracias, Jessika. Mira, lo primero que te diría es, BANXICO yo creo que lo que está tratando de dejar muy en claro es que el SPEI no tuvo problema, y si ponemos la lámina, por favor, bueno, y a lo mejor fue demasiado claridoso, pero está bien, es lo que él tiene que hacer. Como el SPEI no fue hackeado ni vulnerado, pues lo quiere decir muy claro y lo dijo así de claro.

¿Por qué no fue vulnerado? Como ven en la lámina, al SPEI no lo vulneraron, fue en la parte anterior, donde dice conectores, pero cuando entró al SPEI ya venía mal. El SPEI nada más lo transmitió, entonces el SPEI que es donde está Banco de México, pues sí, no tuvo nada que ver; donde dice conectores, pero cuando entró al SPEI ya venía mal, el SPEI nada más lo transmitió.

Entonces, el SPEI, que es donde está Banco de México no tuvo nada que ver; ahora, yo creo que él quería dejar más que claro, por si las dudas, que no tenía nada que ver, creo que a todo mundo nos quedó clarísimo lo que dijo, pues está claro, no fueron ellos, a lo mejor fue rudeza innecesaria, pero no fueron, queda claro que no fueron ellos.

¿Cuántos no cumplieron? Esa es una pregunta que les debe de contestar el Banco de México, porque es el único que la conoce.

Y los 300 millones es una cifra que han dado, ya no sé ni quién. Banco de México, que tiene más información, lo que les diría es lo siguiente, ha habido varios bancos que sí han hecho alguna declaración, algunos bancos que han sacado algún boletín diciendo cómo operan que operan y que no tuvieron problema.

Hubo otro banco que hizo un acto que a mí me parece francamente de un profesionalismo impresionante y mucha calidad y buena entrega a sus clientes, es decir, yo tengo un problema y lo estoy resolviendo. Entonces, si se tarda ni modo, pero yo estoy cuidando su dinero.

Y ese banco sí dijo que tenía un seguro contra fraudes, porque esto finalmente es un fraude, igual que muchos otros. Entonces, quién sabe cuánto de este dinero sea de él, pero el que le corresponda a ese banco que tomó esa decisión no sólo valiente, sino yo creo que muy acertada no tiene quebranto, aparentemente está dicho por ellos, cubierta por un seguro, y además lo hizo muy bien porque es un banco público, es un banco que está en el mercado, entonces es un hecho relevante.

- JESSIKA BECERRA: Marcos, pero no me contestaste. En realidad el Banco de México dice: "Son sus proveedores, ustedes debieron revisarlos, yo ni siquiera autorizo a LG y a PESSA, es culpa de ellos. ¿No tiene el banco como autoridad también parte de la responsabilidad?, ¿no la tiene?, ¿Ustedes reconocen que es culpa de ustedes o sí tiene en parte Banxico culpa?

- MARCOS MARTÍNEZ GAVICA: No, es que yo te diría, el proveedor lo puedes autorizar, el proveedor debe de tener un programa muy bien hecho, pero los programas mejor hechos son susceptibles a ser vulnerados por profesionales que se dedican a eso.

Lo que ningún proveedor de desarrollo de sistemas ni externo ni interno te puede asegurar es que cuando hace un sistema es totalmente a prueba de balas de un hackeo. Y en ese sentido no son culpas. Qué lástima que encontraron esa entrada por ahí, pudo haber sido por cualquier otro lado.

Y creo que Luis quiere agregar algo más.

- LUIS ROBLES MIAJA: Muchas gracias, Marcos.

Simplemente mencionar también que de las cuentas que recibieron los depósitos que posteriormente hubo retiros e intentos de retiro, algunas cuentas o muchas cuentas fueron bloqueadas con anterioridad al momento en el cual se pretendía hacer el retiro; de tal suerte que dentro de todo, yo no quisiera hablar de montos porque, como dice Marcos y lo dice muy bien, la información que existe es la que oficialmente se ha dado por Banco de México y aquí no conocemos las cifras exactas.

Sí hay cantidades que fueron retenidas por los propios bancos. Bancos receptores, es el ejemplo, el banco amarillo que aparece a la derecha.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: La siguiente pregunta, la intervención es de Miguel Ramírez de DNF.

- MIGUEL RAMÍREZ: Buenas tardes. Sería tan amable en explicarnos cuántas fueron las cuentas apócrifas que intervinieron en estos desvíos, también los proveedores dicen que ellos no tendrían nada que ver en eso, sino que es un software que se plantó y esos lo hicieron gente dentro de los mismos bancos.

Y también cuando dice el Banco de México ahorita en un reporte que les pidió una especie de autoría si ya no había algún software dentro de los bancos. No sé si ustedes ya lo reportaron al Banco de México esa información.

Gracias.

- MARCOS MARTÍNEZ GAVICA: De nada, Miguel. Al contrario.

Mira, déjenme tratar de decirles, les queremos dar la mayor información que podamos, sin que inventemos ninguna o tratemos de darles una información de tranquilidad que no esté corroborada.

La ABM no es autoridad, y eso es importante en este momento porque la mayor parte de las veces hablamos por el gremio, pero hablamos de cuestiones de interés del gremio. De este tipo de cosas a la ABM pues no le avisan, tampoco tendrían por qué. Es más no sabríamos no qué hacer con ello, porque no me imagino un banco diciendo: “Oye, ABM te hablo porque tengo un problema que quiero comentarte para que lo manejes.” No, la ABM es una asociación.

¿A quién le tienen que reportar? Al Banco de México o a la Comisión Nacional Bancaria.

Y, por lo tanto, ¿cuántas cuentas? Pues lo sabrá el Banco de México y la Comisión Nacional Bancaria, porque cada banco que detectó cuentas se las comenta a ellos, pero ellos son los que lo tienen, porque además así es, así es como debe de ser. La ABM no tenemos, tenemos información general y esta información que hemos hablado es la que han sacado las mismas autoridades, no nosotros y por eso espero que no sientan que estamos

tratando de ocultar o guardarnos alguna información que quisiéramos compartir. Nos encantaría. No la conocemos.

Y bueno, si alguno de los bancos, podemos hacer, la verdad es que en la mañana les dijimos que, si querían dárnosla y, porque algún banco nos dijo que se sentía muy mal informado, que qué hacía la Asociación de Bancos, se los cuento anecdótico, pero por qué no nos cuentan, nos sentimos desinformados.

Pues no tuvimos más que decirle, “ve a preguntar al Banco de México porque nosotros qué”.

Y sí les hice una encuesta, si querían ahí decirnos, quién estaba, quién tenía un problema y de qué tamaño. Y nadie quiso, no sé por qué.

Perdón pero es así. Entonces, para qué, no queremos confundir. La verdad es no la tenemos y yo también creo que el Banco Central no querrá, por alguna razón revelarlo en este momento.

La tranquilidad, eso sí, ningún cliente ha sido afectado en su patrimonio.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: La siguiente intervención es de Adrián Estañol de CCN Expansión.

- ADRIÁN ESTAÑOL: Hola, buenas tardes. Yo quería saber, mencionaban que los hackeos sucedieron en determinados bancos, en tres bancos, y justamente antes también hubo algunos problemas. Me gustaría saber si piensan hacer algo para poder comunicarse entre ustedes estos hackeos para, con antelación, poder hacer algo, porque al parecer son bancos, el banco sabe y no saben los otros participantes. ¿Se piensa hacer algo en ese sentido?

Otra pregunta sería ¿qué perfil tienen estas personas que retiraban el dinero, que incluso mencionan que las cuentas están congeladas, qué tipo de perfil tenían?

Y en cuanto a los proveedores, a mí me interesaría saber qué tan cerca monitoreaban a estos proveedores, en su caso, en el caso de los bancos es uno solo de los bancos afectados, pero bueno, tienen también otro proveedor, qué tan de cerca monitorean a estos proveedores y sus

certificaciones, porque finalmente BANXICO dice que él no los regula y es cuestión de cada banco tener supervisados a estos proveedores.

Y, por último, me gustaría saber, ¿cuándo le dieron a conocer el problema?, mencionaban que se conoció el hackeo. ¿Cuándo es la fecha que les dan a conocer a ustedes?

Gracias.

- MARCOS MARTÍNEZ GAVICA: Bueno, como les mencionábamos, independientemente de los comités tradicionales de la ABM que funcionan todo el tiempo fue a principios de mayo, que creo que se los dije a principios de la presentación, que nos reunimos tanto con Banco de México, como que se formó un equipo adicional especial para hacer dos cosas:

La primera es, qué medidas tomar para obstaculizar ese modus operandi que estaba sucediendo y que nos dimos cuenta ya de que estaba pasando, que es el que les acabo de mostrar; y de ahí salió la disposición del Banco de México de los montos de más de 50 mil pesos diferirlos un día para su cobro en efectivo, que sigue trabajando, que trabaja solo y después en combinación con las autoridades, primero para matar este problema y, segundo, para pensar futuras medidas que sirvan de evolución de nuestros controles y los controles compartidos con las autoridades para ir al mismo ritmo que vienen los hackeadores y va a ser permanente.

El perfil de las cuentas congeladas cada banco está viendo en su banco qué cuentas fueron y evidentemente hubo aperturas que a la primera pasaron, pero que a la segunda ya no pasaron, y es a lo que se refería Luis con cuentas congeladas, porque las mismas políticas de lavado de dinero de los bancos vieron comportamiento irregular, que lo tienen los sistemas de los bancos y las congelaron.

Entonces, ahí hay dinero que no sabemos cuánto es, que salió de la Tesorería de uno de los bancos, pero que ya no se fue a la calle, que está regresando al banco porque se quedó el dinero congelado en la cuenta.

Hay algún banco, pero les voy a contar anécdotas, porque como les digo, algún banco que lo que comenzaron a hacer cuando vieron ese comportamiento atípico no es muy normal que te abran una cuenta y al día siguiente te llegan a retirar 100 mil pesos en efectivo; que cuando les pedían

información adicional para corroborar identidad, en fin, iban corriendo y ya nunca regresaban.

Entonces, todo lo que hablemos son anécdotas, la cifra esa en todo caso son 300 millones, puede ser menos; y los proveedores, es que este pobre proveedor ya me imagino cómo la ha de estar pasando, es que cuando contratas a un proveedor tienen certificaciones de calidad y de buenas prácticas, de muchas cosas, porque son temas muy delicados.

Lo que ningún proveedor te puede comprometer y que le creas es que nunca lo van a hackear o que su programa es inhackeable; igual que si alguno de los directores de tecnología de sistemas, de cualquier negocio, les dice a sus jefes, que le asegura que a él no lo van a hackear, yo no lo contrataría; porque de entrada es un mentiroso. No puede asegurarte que no lo van a hackear.

Sí te tienes que asegurar de que sea lo menos vulnerable posible. Y en ese sentido actuamos todos.

- ALBERTO GÓMEZ ALCALÁ: Le comentaba ahorita al Presidente que lo que acordamos en la reunión de hace un rato, fue que vamos a hacer una inversión millonaria para tener una plataforma de comunicación anónima para delatar inconsistencias que cada Banco perciba y que tratan precisamente de atacar este tipo de problemas.

Cuando vemos algo inusual, que no entendamos, en ese momento lo podamos reportar sin decir quién es el Banco, sin decir quién es el cliente, respetando la información, pero que esté alertado el sistema.

Y eso nos va a implicar una inversión millonaria que hoy acordamos con los asociados, y la vamos a hacer ya a la brevedad.

- ADRIÁN ESTAÑOL: ¿A quién la estarían reportando?

- ALBERTO GÓMEZ ALCALÁ: Entre nosotros. Es una plataforma de comunicación entre el sistema.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Jeanette, por favor, te pedimos tu intervención.

- JEANETTE LEYVA: Sobre esto mismos que acabas de decir ahorita, Alberto, ¿no tendría nada que ver con el GRI, con este grupo que va a crear la Comisión Nacional Bancaria y de Valores de mandar informar, o sería otro, sería distinto a esta base?

Tengo un par de preguntas. Si bien ya nos queda claro Marcos, que dicen que vayamos a Banco de México y preguntemos con más precisión cómo va, aquí hay cuatro Directores o Presidentes de Bancos, y a mí me gustaría preguntarles una:

¿De forma individual, a ustedes les avisaron, o quién les avisó o cómo se enteraron precisamente de este hackeo? Tomando en cuenta que el mayor fue el 26 de abril y 13 días después, hasta el 8 de mayo, Inbursa fue atacado nuevamente hasta con el mayor monto sustraído. Pasaron 13 días. ¿No se prepararon, no les avisaron? ¿Hizo falta esto que mencionan, la comunicación de revelar que algo estaba sucediendo?

Con respecto a las contrataciones de los empleados y demás, Banco de México no descarta que haya empleados bancarios involucrados, como ya preguntaron hace un momento. ¿Estarían ustedes reforzando las contrataciones, la forma y el perfil de quiénes están, tanto en área de Sistemas, como en área de Casas? Porque parece que ahí está la confabulación entre delincuentes y empleados de la banca.

Otra pregunta más sería. Nos queda claro que la imagen de la banca fue dañada con todo esto, aunque no hay clientes afectados, no les perjudica más que los socios no reconozcan este hecho y que por el contrario lo sigan negando al menos públicamente, y aquellos que cotizan en Bolsa solamente uno ha hecho un aviso de manera muy general.

¿No perjudica esto y no daña más la imagen del sistema, el no reconocer que fueron atacados?

- MARCOS MARTÍNEZ GAVICA: A ver, la comunicación. La comunicación informal es la que está siendo reforzada. La comunicación entre distintos bancos es diferente dependiendo la relación que llevan entre ellos.

Obviamente no está regulada, pero son de las cosas que como, con medidas como las que mencionaba ahora Alberto, estamos tratando que en beneficio de todos tengamos una comunicación más fluida y yo te diría,

afortunadamente como ahora vemos que fue un problema muy importante en cuanto a atención de clientes.

Pero afortunadamente no de gran magnitud ni en términos económicos ni en el número de participantes que estuvieron afectados, bueno, pues ahora queda claro que tendremos que encontrar unos mecanismos para que los negocios no tengan un mayor temor de que nadie diga “tengo un problema” y eso acabe siendo como consecuencia que sea un banco al que la gente le comience a tener temor o que algún competidor comience a sacar alguna ventaja.

Creo que a estas alturas queda claro que esas prácticas no deben de ser.

Queda claro que, puedes tener miedo, pero lo peor es que tengas un problema mayor.

En esto ya estamos trabajando. El pasado, pues qué te puedo decir. Si hay empleados involucrados, no lo sabemos. Es difícil pensar que no hay nadie involucrado, pero tampoco podemos como Asociación de Bancos asegurarte que hay alguien, descartarlo, no podemos, pero tampoco asegurarlo.

Y la imagen, sí, nos preocupa la imagen, por supuesto. Por eso dijimos que el riesgo reputacional es lo que más interesados nos tiene para esta conferencia de prensa, y por eso es que les decimos que:

Punto número 1: ningún cliente fue dañado, más que en su tiempo de servicio, pero patrimonialmente ninguno.

Que nos sentimos que es suficientemente grave afectar el tiempo de servicio de la banca que ha evolucionado y ser de lo más eficiente del mundo, pues sí, nos parece gravísimo, pero que nos parece que fue necesario, para que no se volviera grande, pues entonces valió la pena y lo que esperamos es que se resuelva lo antes posible y que regresemos a esa práctica de ser de los sistemas financieros más eficientes y rápidos del mundo.

- ALBERTO GÓMEZ ALCALÁ: Nada más una aclaración, Jeanette, porque las palabras son importantes.

Realmente no estamos un ataque a la banca, el SPEI es como la carretera, los coches son los bancos y aquí lo que falló fue un semáforo, que en lugar

de ponerse rojo dio verde, pero realmente no sufrimos un ataque a la banca, independientemente de lo que ya señaló Marcos, de que el tema del hackeo es una preocupación permanente de cada uno de los asociados de la banca.

Aquí estamos hablando de un terreno que está fuera de la banca, que es la conexión, que es como el equivalente al semáforo que decía, pero realmente la banca no es aquí la víctima de ese hackeo. Yo creo que es importante ahí el término, porque realmente este ataque no es a la banca, es al semáforo, el flujo de las transacciones.

- EMILIO ROMANO MUSSALI: Yo quisiera agregar, Jeanette, lo que estás mencionando, por ejemplo, en términos generales yo creo que todo esto se resume de una manera.

Sí logramos, primero empezar por reiterar lo que está diciendo nuestro presidente, otra vez de que el Sistema de Pagos de México, el SPEI, es un sistema que no lo hay prácticamente a nivel mundial, o sea, que estamos nosotros en la vanguardia de los pagos de inmediato, las transferencias de inmediato a nivel de personas físicas y personas morales en la red bancaria; o sea, que la banca mexicana tiene un sistema de pagos muy sofisticado.

Segundo, que los ataques cibernéticos ocurren en todas partes del mundo y es una carrera continua entre los hackers, los defraudadores y la banca, y la tecnología de la banca, y nuestro reto es que siempre tenemos que estar un paso adelante, y ese va a ser un reto que vamos a tener que vivir si ya ahorita no, y ustedes lo viven, digo, todas sus computadoras y demás, no es un tema exclusivo de la banca, no es un tema de la industria, es un tema de todas las industrias.

Entonces, ese es nuestro nuevo mundo que vivimos, es que estamos en un mundo que siempre tenemos que estar un paso delante de quién quiere utilizar la tecnología para robar información, dinero u otras cosas, y generar algún daño.

Tercero, sí hubo información, de hecho la banca teníamos sistemas alternos, se recurrió en los sistemas alternos, se comunicó, se tomaron precauciones, se contuvo el efecto, y lo más importante de todo esto es que se logró no solamente contenerlo, pero tenemos ahora un caso de estudio muy interesante, que es un poco lo que decía Marcos con el estudio forense, que es que ahora nos toca a nosotros, a la autoridad, a cada uno de los bancos,

a la ABM, y a toda la integración del Sistema Financiero, encontrar las mejores prácticas, encontrar dónde podemos actuar mejor, dónde podemos protegernos más.

Entonces, lo que sí van a encontrar no es una industria que les pueda decir que estamos perfectamente a prueba de un ataca, pero lo que sí vamos a encontrar es un incremento muy importante en la fortaleza de los sistemas y de los procesos de comunicación de, decías tú, por ejemplo, de contratación de personal, todos esos temas, todos los protocolos de personal, todos los protocolos de ciberseguridad, de contratación de proveedores, de terceros para que hagan sistemas operativos para la banca.

Todo esto, este incidente nos permite encontrar dónde podemos ser mejores y lo vamos a instrumentar conjuntamente, podemos comunicar mejor como gremio, la autoridad por actuar de una manera más eficiente y más inmediata; todo eso nos está dando este incidente como un ejemplo claro de cosas que podemos hacer mejor.

Entonces, si bien pasó este incidente, que como bien lo dice Alberto, es un incidente que no es un ataque general a la banca, es un incidente que sí nos permite encontrar cómo poder mejorar de manera muy importante la seguridad de los sistemas, la robustez del Sistema Financiero Mexicano.

Y desde esa perspectiva ese es el lado bueno que le vemos al efecto o al incidente que hemos sufrido en estos meses.

- LUIS ROBLES MIAJA: Creo que hay una reflexión también aquí que cabe hacer, y perdón que ya ustedes me califican como el optimista Robles, pero bueno.

No, hay que ver un dato primero, que no hemos tenido oportunidad de compartir. El SPEI es de los pocos o el único sistema de pagos que trabaja en T, es decir, una transferencia el mismo día prácticamente con montos, cualquier monto, y con costos bajísimos, lo cual permite realmente bancarizar, bajar los costos de los usuarios, etcétera, que es un punto positivo.

Segundo punto positivo, el SPEI no fue vulnerado, el SPEI como tal está limpio; quien fue vulnerado ya vimos que ya lo explicó el Presidente con mucha precisión. Entonces, también es de las cosas buenas, o sea, tenemos

un sistema que no fue vulnerado, tenemos un sistema que es de los mejores del mundo y tenemos un sistema que sus costos de transacción son bajísimos. Y eso creo que hay que resaltarlo, porque a veces vamos a las partes negativas y pocas veces sé que no es nota, pero pocas veces he tocado los positivos.

- MARCOS MARTÍNEZ GAVICA: No, sí es nota.

- LUIS ROBLES MIAJA: Pues sí, yo digo que sí, pero ellos.

- MARCOS MARTÍNEZ GAVICA: A ver qué piensan ellos, pero...

- LUIS ROBLES MIAJA: A ver qué piensan ellos.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Margarita Jasso de La Crónica.

- MARGARITA JASSO: Buenas tardes, Margarita Jasso del periódico La Crónica. Algunas precisiones. Una, si bien nos mencionaban la inversión millonaria que van a hacer para este sistema de comunicación entre todos los bancos, por lo menos para tener una idea de cuánto es esta inversión millonaria que se está hablando, por lo menos un alrededor para tener una idea de cuánto estamos hablando y si son todos los bancos que operan los que van a participar en esto.

Luego sí me gustaría una respuesta muy puntual a esta queja del Banco de México de que los bancos contratan a proveedores no certificados, así fue como su queja o reclamo, porque entendí el mensaje de que los proveedores no pueden ser inhackeables, pero ellos se refieren a no certificados. Entonces me gustaría muy puntual la respuesta. Qué le responderían a la autoridad.

Me gustaría, si tienen algún dato de que este tipo de modus operandi que ya nos explicaron, si se ha replicado en otros países tal cual así fue, y si tienen el dato, como referencia, en dónde se ha encontrado tal cual fue.

Y me salgo un poco del tema para preguntarles, es la última conferencia de prensa con ustedes antes de las elecciones, y ya llevamos dos debates presidenciales en los cuales hay quejas de que no hay propuestas económicas puntuales y me gustaría saber por parte de la ABM cuál es la

petición, la queja o la solicitud que le hacen a los candidatos, previo a las elecciones. Gracias.

- MARCOS MARTÍNEZ GAVICA: Bueno, como les mencionamos, lo que los bancos gastan, han gastado históricamente, incluso antes de este evento, en temas de seguridad, ronda alrededor de los dos mil 400 millones de pesos.

Este sistema todavía no lo tenemos cuantificado porque estamos todavía estudiando el alcance y dependiendo de qué tanto queramos ir, nos lo van a cotizar.

Sí hay antecedentes. Evidentemente esta no es una banda que nació en México para los mexicanos, nacen, andan por otros lados y ahora, pues encontraron aquí, están todo el tiempo viendo dónde pueden y encontraron esta vulnerabilidad, pero hay un caso parecido en España y fue un caso en el que la forma en que se detuvo tuvo que ver con que detuvieron a varios de los señores que hicieron los retiros y los metieron a la cárcel.

Entonces, no fue desmotivando al hacker, sino desmotivando a los cómplices que retiraron el dinero. Y ojalá aquí podamos tener alguna novedad, le toca a cada banco hacer las denuncias y perseguirlo con la PGR, pero si no hay mejor solución que saber que si te prestas a eso puedes acabar en la cárcel.

Y nosotros en la Convención Bancaria, si recuerdan les hablamos de un decálogo, de cuáles pensábamos que nuestra experiencia después de varias crisis que sirvieron para que el sistema financiero sea lo sólido que hoy es en nuestro país, nos sirvieron como las cosas que hay que hacer y las cosas que hay que evitar.

Entonces, ya se los dijimos, ya les dimos una vuelta con ustedes hace un mes, se las podemos volver a mandar para tenerlas frescas, pero está dicho, es eso mismo, ese decálogo que presentamos en la Bancaria y que con mucho gusto se los hacemos llegar de nuevo.

- MARGARITA JASSO: Perdón, me faltó el tema de los proveedores, y respecto a estas personas que fueron involucradas en los retiros, yo sé que es labor de la autoridad y en eso están para hacer este análisis, ¿pero

ustedes tendrían un aproximado de cuántas personas pudieron haber participado en el retiro de ese dinero, de estos cómplices que mencionan?

- MARCOS MARTÍNEZ GAVICA: Nosotros no, cada banco tiene que é cuentas abrieron, pero no cuántas gentes fueron a retirar.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Tenemos tres intervenciones más.

Stephanie Eschenbacher, de la Agencia Reuters. Y perdón si pronuncié mal tu apellido.

- STEPHANIE ESCHENBACHER: Quisiera saber por favor qué tipo de sanciones podrían enfrentar los bancos que fue puesto el sistema en peligro, y si hay antes ese tipo de sanciones.

- MARCOS MARTÍNEZ GAVICA: No, ninguna de las dos cosas tenemos respuesta.

- EMILIO ROMANO MUSSALI: Pudiera yo nada más agregar algo.

El sistema, en peligro no se puso el sistema, obviamente pasó un incidente y como ya lo platicamos, pero lo que es muy importante es lo que decía nuestro señor Presidente, es que no se nos olvide acá que el malo no es la banca, ni las autoridades, el malo son los grupos delictivos que están operando con impunidad.

Estamos hablando, por ejemplo, es un caso concreto, hace día robo de ferrocarriles, digo, una solución puede ser hacer ferrocarriles, vagones blindados, esa puede ser una; la otra es agarrar y meter a la cárcel a la gente que se está robando los ferrocarriles, que no es normal. Eso se nos olvida.

El robo de gasolina igual, pues ahora vamos a mandar la gasolina en tanques blindados por vía terrestre en lugar de gasoductos o gasolinoductos o como se llamen. Pues eso es absurdo. O sea, tenemos que tener un país donde a los malos se les meta a la cárcel.

Entonces, lo que sí creo que sí podemos ver es que la forma más fácil de garantizar que estos incidentes se van a repetir, de diferente manera y no

necesariamente en la industria financiera, en otras industrias, es el que la gente esté impune, con el beneficio de un robo en la calle, feliz y contento.

Entonces, yo sí quisiera resaltar que aquí la misión como país y como mexicano, es insistir en el cumplimiento de las leyes y que la gente que roba se vaya a la cárcel, es la forma adecuada de solucionar todos estos problemas.

Y la banca, ciertos bancos, han sido víctimas de este tipo de fraude, que debe ser perseguido y las leyes se deben de aplicar con las consecuencias legales que eso implica.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Lupita Flores, de Televisa, por favor.

- GUADALUPE FLORES: Buenas tardes. Bueno, yo tengo también tres preguntas. En el comunicado de Banco de México se responsabiliza en general, a la banca en general, por haber vulnerado al Sistema Financiero en general por estas tres instituciones que ustedes mencionan.

Mi pregunta es: Entonces, ¿la ABN deslinda a toda la banca y solamente focaliza el problema en estos tres bancos?

También en el comunicado se habla de que la regulación fue heterogénea, que lo cumplieron de manera heterogénea. ¿Quiere decir que, entonces, se le debe de sancionar a estos tres bancos, porque le está afectando a la imagen de toda la banca? ¿Ustedes qué opinan de sobre ello?
También quiero preguntarles que dentro de las negociaciones del Tratado de Libre Comercio, Canadá propuso que la banca de los tres países compartiera bases de datos y creara una especie de SPEI para las operaciones.

Entonces, después de este incidente, ¿es conveniente? ¿Cómo quedó? Porque se ha sabido poco de las negociaciones del TLC en materia financiera. ¿Sería conveniente tener un SPEI regional o una cosa así?

También un aspecto técnico. Yo tengo información de que tres bancos no trabajan con SPEI, que tienen sus propias plataformas y se conectan y hacen operaciones con otro tipo. ¿Qué hay en esta materia?

Y, por último, ¿hay algunas personas que están solicitando que vuelva la Policía Bancaria después del asalto que hubo a una sucursal, en donde los delincuentes ya están asaltando a los cuentahabientes que están sentados ahí. ¿Qué está pasando con estos asaltos ya en sucursales? Gracias.

- MARCOS MARTÍNEZ GAVICA: Nosotros leímos o interpretamos distinto el comunicado, como decía, del Banco de México. Nosotros lo que entendimos es que lo que quiere dejar muy claro es que el Banco Central y su SPEI no tienen problema y que no tuvieron problema. Lo cual creo que ya nos queda claro a todos. Y yo me quedaría con ese como el mensaje, más que el otro, que fue una forma de decirlo.

En las sanciones, no es más que un tema entre las autoridades y cada uno de los bancos.

En el TLC hablando del tema que hay, no es el SPEI porque si fuera el SPEI tendrían que tener algo como lo nuestro que no lo tienen, tienen algo bastante más limitado, como les decíamos, que está limitado a instituciones financieras no a clientes, y a los grandes bancos, no a todas las instituciones.

Y sí, hay 48 bancos en el SPEI, y quién sabe quiénes serán los tres que…

- GUADALUPE FLORES: Es que no hay iniciado operaciones.

- MARCOS MARTÍNEZ GAVICA: Ah, es que no han iniciado operaciones, son los tres que están aprobados, pero no han iniciado operaciones.

Y de los asaltos, qué fue.

- GUADALUPE FLORES: Hay algunas personas que están pidiendo que vuelva otra vez la Policía Bancaria afuera de las sucursales, o dentro de sucursales después del video que vimos, donde un grupo de delincuentes entra y asalta, ya no al banco, porque muchas operaciones son electrónicas, en fin. Pero ahora el cliente está vulnerable en las sucursales. Qué harán para reforzar la seguridad en las sucursales bancarias. Gracias.

- LUIS ROBLES MIAJA: Si me permites, Presidente. Desde el año de 1904 o 3, y posteriormente en el año de 2016, se han firmado sendos convenios con el Gobierno de la Ciudad de México, este último justamente para proteger al cuentahabiente bancario.

Los bancos hemos adoptado una serie de medidas que van desde, por ejemplo, la instalación de cámaras en los estacionamientos, monitores para que no haya gente que no tiene nada que hacer en la sucursal viendo temas, y esto como lo dijo el Jefe de Gobierno en una entrevista, el anterior Jefe de Gobierno en una entrevista que dio hace aproximadamente seis meses, algo así, produjo una reducción, no recuerdo la cifra Lupita, pero una reducción no menor de los asaltos a cuentahabientes.

No se diga de las sucursales bancarias.

De tal suerte que yo creo que ese video tan, pues tan dramático a que te refieres, no es de ninguna manera una tendencia, una constante y a los que más nos duele es a nosotros que algunos de nuestros clientes sean afectados por los malos.

No sé si.

Mejor policía cibernética, efectivamente.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Y concluimos este ciclo de pregunta con la intervención de Agustín Vargas, de la Revista Hábitat.

- AGUSTÍN VARGAS: Buenas tardes. Ingeniero, debido a la magnitud de este convenio que se firmó y de este protocolo para la ciberseguridad, y la convocatoria que tuvieron con las autoridades, que también es algo muy importante, este tema o más bien este asunto, no el incidente como tal, sino el asunto de la ciberseguridad, ¿ya se está tratando o podría tratarse ya como un tema de seguridad nacional? Eso, por un lado.

Y, por el otro, ¿creen ustedes que algún día van a conocer no exactamente lo que pasó porque ya ustedes lo presentaron gráficamente, sino cómo ocurrió y quiénes participaron y si lo harían público ustedes en determinado momento para revertir precisamente esa mala imagen que se ha proyectado del Sistema Bancario Mexicano?

Es todo, ingeniero.

- MARCOS MARTÍNEZ GAVICA: Mira, yo no sé si vamos a acabar o van a acabar encontrando los bancos afectados a los hackers, a los actores intelectuales que muy probablemente no están en México.

Sé que sí vamos a acabar o van a acabar estos bancos dando, o los bancos que tienen operaciones hechas de retiro, cuentas abiertas y retiro, ahí sí hay una expectativa de que acaben agarrando a varios, no a uno, sino a varios, con lo cual estará la desmotivación para que alguien más se preste, que de momento parece que está estacionada la operación.

Lo de los hackers lo importante, más que agarrarlos, que no es nada fácil, es que volteen para otro lado porque aquí ya se les acabó ese juego, o busquen otra forma, ya que Brasil está más fácil en este instante porque encontraron algo y se vayan para allá. Entonces, como el chiste, no es que corras más rápido, nomás más rápido que el vecino.

Pero finalmente de eso se trata, y como les decimos, las partes estas de ciberseguridad sin duda, en todos los países tiene que ser seguridad nacional y yo no creo que apenas vaya a ser, yo creo que es una parte importante de seguridad nacional que la tienen muy consciente y en las distintas industrias también.

- JOSÉ MIGUEL DOMÍNGUEZ CAMACHO: Muchas gracias a todos por su presencia.

Ahorita les van a repartir copia de la presentación para su consulta.

Muchas gracias a todos.

- - -o0o- - -