83 CONVENCIÓN BANCARIA

"PROSPERIDAD PARA TODOS EN LA ERA DIGITAL"

Versión estenográfica **Acapulco, Gro., 13 de marzo de 2020**

Conferencia "Cybersecurity: A Business Differentiator"

- MAESTRA DE CEREMONIAS: Damos la bienvenida a Michael Chertoff, ex secretario de Seguridad Nacional de los Estados Unidos de América.

- HON. MICHAEL CHERTOFF: Buenos días todos. Hoy estaré hablando a ustedes en inglés, obviamente me invitaron para estar aquí con ustedes y yo sospecho que es un evento público en el que voy a estar participando durante muchos años.

Como saben que hay cosas que se saben es interesante en una época en que cada vez más personas están tratando de limitar su interacción física, cada vez a pasar a estar en línea del camino digital, en un momento en que cada vez pudiéramos no querer estar en contacto físico durante cierto tiempo.

Para poner las cosas en perspectiva, hemos visto el elemento digital de Fintech y de banca, que se ha disparado dramáticamente en años recientes.

Es difícil recordar que hace aproximadamente 15 años solamente el 15 por ciento de la población del mundo utilizaba la Internet, y en términos de banda ancha móvil solamente el 3 por ciento se suscribió en un mundo de desarrollo.

Por lo tanto, estábamos hablando de una minoría muy grande de la gente. En la actualidad más del 50 por ciento de la población mundial tiene acceso a Internet, y esto va a incrementarse exponencialmente en un mundo en vías de desarrollo, la banda ancha, móvil han llegado al 60 por ciento, de tal manera pueden ver ustedes cuál es el cambio tan rápido que se está llevando a cabo.

Nos sorprende que eso ha causado consideraciones muy serias viendo cómo el modelo digital puede ser utilizado para extender la banca a los no bancarizados, aquellos que no tienen sistemas bancarios adicionales.

El Banco Mundial, por ejemplo, dice que los servicios digitales financieros se han lanzado en más de 80 países con cientos de millones de gentes que previamente nunca habían tenido la posibilidad de interactuar con un banco, y es especialmente en el hemisferio sur del mundo.

Hay beneficios enormes asociados con ese movimiento a Fintech y banca móvil, hay una reducción en esa comunidad no bien atendida, solo que esto ocasiona o da mayor acceso para empezar con pequeños negocios en todo el mundo, y significa que hay acceso a otros servicios financieros, como seguros y asesoría financiera.

Para los gobiernos el tornarse digital también tienen beneficios, ya que reduce los robos bancarios en los bancos físicos y da herramientas adicionales para combatir el lavado de dinero y la corrupción.

Tal como se ha observado, México ha sido el líder en adoptar la banca de las iniciativas del futuro. El 28 de marzo de 2018 se convirtió en un país que aprobó

la Ley de Fintech, que tiene un marco legal para que las compañías ofrezcan acceso alternativo para financiamiento y opciones para pago de créditos financieros.

Se han reducido a muchos mexicanos que no eran bancarizados como resultado. México se ha convertido en un líder regional con más de 273 acciones de Fintech que están en operación.

Yo sé que eso es muy bueno, ha sido una iniciativa de la administración actual de México para la banca. Se distribuye en todos los rincones de México por supuesto que digital puede ser uno de los principales componentes en este esfuerzo, pero también hay un riesgo. Y el riesgo es el siguiente: cada vez va a haber un mayor y un pacto que los ciberataques puedan tener en nuestros sistemas financieros, y esto es algo que requiere la atención de todo mundo, ya que en el foro en la dispersión del *Fintech* lleva a cabo en el resto del mundo.

Cuando pensamos en este riesgo estamos pensando en cuáles son las amenazas de cuáles son las vulnerabilidades y cuáles son las consecuencias, obviamente esto suma alta frecuencia a aquellos que están viendo este asunto y atendiéndolo.

Vamos a tomar un momento cuando hablemos de las amenazas para discutir los diferentes actores amenazantes que vemos y algunos de los cambios que también hemos visto en años recientes. No es sorprendente, gran parte de la actividad criminal o de la amenaza de la amenaza de la actividad en internet, especialmente en lo que se refiere a bancos e instituciones financieras proviene de criminales.

Conforme al Internet pasa de ser un experimento y se convierte en una empresa o plataforma empresarial, los criminales empezaron a darse cuenta que podían cometer crimen y obtener dinero a través del internet, es como la famosa historia del que robó bancos en Estados Unidos, a *Willie Sutton* se le preguntó: “¿Por qué robas a los bancos?” “Porque ahí está el dinero, pero el dinero ahora está en el Internet”. Y eso es lo que afecta a los criminales. Lo que se necesita es la escala de lo que está sucediendo.

Es posible ahora robar millones de dólares en un día, previamente la gente iba a los cajeros automáticos, la compañía que estaba haciendo el *software* de las ADN en la India y pudieron alterar en muchas máquinas que estaban en el mundo y en un sólo día tenían a personas que salían a estos diferentes bancos y

retiraban todo el efectivo que estaba en el banco y ganar millones de dólares en un sólo día; por lo tanto, en la escala de la criminalidad realmente es dramática.

Parte de lo que estamos viendo es lo siguiente, por ejemplo los estados-nación están entrando a este país; Carolina del Norte tiene mucho de su economía robando dinero, por lo tanto, en 2016 algunos de ustedes recordarán que el banco se robó su cuenta de bancos, 81 millones de dólares del banco de Nueva York se había transmitido ese dinero a diversos beneficiarios, el esquema era robar 1 mil millones de dólares, pero había un error de ortografía y uno de los empleados, un ser humano lo notó y dijo: “Hay algo curioso en esto”, y trató como que dio alarma y se detuvo, de cualquier manera había robado 80 millones de dólares.

Las Naciones Unidas han estimado que los ataques contra los bancos y las instituciones de criptomonedas, el banco de Corea ha llevado al robo de dos mil millones de dólares que están siendo utilizados para comprar armas de destrucción masiva, eso les da a ustedes una idea de la escala de esto.

Más reciente y más perturbador para los bancos y otras instituciones que se basan en los datos es el cobro de los rescates, básicamente los datos están encriptados, dice: “recibí un mensaje que si no pagas este rescate, la persona va a desaparecer y no vas a tener los datos para los bancos, que están muy preocupados por la confidencialidad de las cuentas, de los datos, la disponibilidad de sus procesos de negocios, y la integridad de los datos”.

Esta es una amenaza muy importante y yo creo que vamos a ver mucho más de esto.

También, hemos visto y tengo que decirlo, un incremento en que los bancos son el piso de batalla de los juegos geopolíticos y esto puede afectar a los países nación.

Por ejemplo, en 2011 a 2013, los ladrones iranís tuvieron un ataque sustancial contra los bancos americanos, como venganza de lo que consideraron que era un ataque de los americanos a los embarques iranís.

En 2007, recordarán ustedes que los rusos atacaron a Ucrania, perdón, Estonia y cerraron las agencias gubernamentales y los bancos durante un periodo determinado.

Más recientemente, la Ucrania fue una víctima de estos ataques y se llevó a cabo un programa de contabilidad que estaba siendo bajado por las empresas en toda Ucrania, incluyendo empresas de otras partes del mundo que tenían oficinas en Ucrania. Esto costó cientos de millones de dólares para estas compañías.

Commermercer es la compañía de medicamentos. Vamos a ver cada vez más, no solamente a los grupos criminales, pero los países nación que entra a este negocio de atacar a las instituciones financieras por motivos geopolíticos.

Y esto significa la emergencia de la seguridad de esa situación es mayor aún.

¿Cuáles son ese tipo de cosas que tenemos que estar considerando en términos de prepararnos en cuanto a nuestras vulnerabilidades se refiere?

Algunas personas ven en la red, en que la seguridad debe funcionar, es como los franceses trataron la seguridad, Alemania, en los 40s, protegieron, construyeron muchos puentes para evitar la *línea Maginot.* Este enfoque funciona, más o menos en ciber, al igual que funcionó para los franceses, en 1940, quiero decir que no funcionó, no, para nada.

Tenemos que ver más la lista de dónde está red. Básicamente esto tiene que ver con todo un rango de remedios y herramientas que tiene que distribuirse.

Voy a empezar con el hecho en que mucho esto tiene que ver con educación de la gente. Es interesante pensar que muchas personas atribuyen los ciberataques a una manipulación muy sofisticada del código de personas que estaban diseñando este malware y es así como se puede preparar las defensas.

Y hemos visto muchos casos de intrusiones debido a errores humanos sencillos, alguien le dio clic a algo que tenía software malicioso.

En el caso de *Petya* las víctimas de ese ataque se dio, fueron entidades y empresas y personas que no habían aplicado un parche que *Microsoft* tenía disponible con tiempo, pero que si no lo podías, esa va a ser una vulnerabilidad.

Entonces, la crisis de marzo se pudo haber evitado, pero la gente no parchó el sistema y tampoco no actualizaron. El no actualizar es un problema muy serio.

Y otras cosas que tenemos que considerar son las siguientes: la identidad es una de las partes de seguridad más difíciles y más débiles en cuanto a los ataques.

Cada vez vemos más y más ataques que no tienen que evadir virus o capacidades antivirus o defensas, sino lo que vemos es gente, les roban sus credenciales. Si alguien se enmascara y tiene el acceso correcto entra a la red y entonces comete los daños.

Y esto se hace porque la gente muchas veces tiene contraseñas mal protegidas o contraseñas que son fáciles de descifrar o porque cada vez más es posible hacer investigación en línea sobre personas que te va a dar idea de cómo puedes autenticar su identidad.

Creo que nosotros cada vez lo vamos a ver más y más, y esto es un enorme reto en el futuro.

¿Por qué? Porque al empezar a autentificar y muchos bancos lo requieren para transacciones grandes, tenemos que tener una llamada telefónica o una autentificación de voz, además de la instrucción por correo electrónico.

Cada vez vamos a ver voces sintéticas que van a imitar a la gente de manera sofisticada.

Vamos a seguir pensando en cómo protegemos la identidad en un ambiente dinámico, a donde los malos cada vez están pensando en nuevas maneras para explotar lo que estamos haciendo ahora.

Otra de las cosas que quiero mencionar antes de darles a ustedes un panorama más general, una de las cosas que escuchamos es la inteligencia artificial.

La inteligencia artificial puede ser una herramienta en las manos equivocadas, y eso es muy peligroso. Se puede usar para averiguar cuál es la contraseña de una persona o para averiguar otros elementos de su conducta o de sus antecedentes que se pueden explotar, pero también puede ser un mecanismo de defensa, porque si nosotros vemos los activos clave que están bien protegidos y bien resguardados en la red y monitoreamos la red para ver conductas que sean anómalas o para ver conductas cuestionables, esto resulta señal de alerta de que alguien va a querer hacer algo y hay que ponerle atención.

Entonces, tienen que estar enfocados en ese tema.

La inteligencia artificial, como todo lo demás, tenemos que ver los riesgos que van a ser algo de beneficio, entonces vamos a hacer un par de observaciones generales antes de pasar a la sesión de preguntas y respuestas.

Primero, la ciberseguridad, como decimos en Estados Unidos, es un deporte de equipo. En el mundo financiero la mayoría de los activos están en manos de bancos privados y mucha de la carga de la seguridad va a estar impuesta por las instituciones bancarias y financieras que tienen que proteger a sus clientes, tienen que proteger sus datos y sus activos. Sin embargo, no lo pueden hacer solos, requieren la cooperación de los clientes y también requerimos la cooperación del gobierno, y el que todo mundo esté en la misma página es crítica.

Si tus clientes no se preocupan de las contraseñas o son descuidados o no usan higiene cibernética, pueden ser el camino para meterse a su red, que va a ser un problema muy serio.

Al mismo tiempo, el gobierno, aunque el gobierno no va a ser sentado en tu red y no va a defenderte, también puede compartir información sobre amenazas, puede alertarte, puede trabajar de manera coordinada y compartir información sobre las mejores prácticas e incluso puede trabajar de la mano con los bancos privados.

En Estados Unidos una comunidad de servicios financieros es la más avanzada para integrar a sus actividades de cibercolección y entonces eso claramente es algo que requiere no solo que los esfuerzos del sector público, sino también del privado y también del público.

Lo que se requiere no es sólo dinero, lo que está en juego no es sólo el dinero, sino la confianza pública en el sistema financiero.

Se acuerdan del 2008 y del 2009, todos lo recordamos y además del problema de liquidez que se tuvo y que erosionó en esa época, tuvimos una gran crisis de confianza y fue muy importante en ese momento que los bancos se reunieran y que el gobierno como equipo trabajaran para dañar de manera limitada y para que la gente siguiera teniendo confianza en el sistema bancario, si no hubiéramos tenido resultados innombrables.

También hubo un resultado importante o reporte que salió de la Reserva Federal que analizó como ciberataque, puede causar una crisis de liquidez, si los bancos críticos pierden acceso a ver qué activos tienen, qué pagos están entrando,

pueden hacer que no se hagan pagos hacia afuera y puede tener un efecto en onda hacia otros bancos que se va a afectar la liquidez y cosas que pensaron que iban a entrar no entraron. Por ello, tenemos un efecto de cascada y eso me lleva el último punto que quería hacer antes de pasar a la sesión de preguntas y respuestas.

Uno de los elementos en ciberseguridad que no se discute mucho y que no es glamurosa y que realmente no es fácil de detectar es la resiliencia. Se implica, por lo que acabo de mencionar hace unos minutos sobre el 2008 y 2009 la capacidad de ser resiliente, a menudo es la diferencia entre un día muy malo y un día catastrófico, es la resiliencia, es algo en lo que tenemos que planear qué hacemos y de hecho la disponibilidad no se puede permitir a través de los impuestos o si los datos se corrompen. Entonces, la manera para compararlo es planear y ejercer.

Hace unos años yo trabajé con un banco global, que no voy a mencionar su nombre en un ejercicio con los siguientes escenarios. Qué pasaría si su proveedor, su tercero para identificar a los clientes anuncia: ¿saben qué?, todas las contraseñas y todo lo que hemos hecho para identificar a los clientes se comprometió por grupo criminal, no podemos confiar en él, y la reacción de los bancos es vamos a tener que cerrar la operación, no vamos a pagarle a nadie hasta que averigüemos de manera alterna de validar a nuestros clientes. Pero al trabajar esa discusión, al observarlo les dijimos tiene muchos clientes que obtienen pagos y retiros de manera constante a las mismas personas que pagan cada dos semanas, por ejemplo, para nómina. Esa es la opresión estándar.

Para ese tipo de cosas van a poder seguir haciéndolas sin irrupción, prácticas ordinarias, aunque hubiera una pregunta relativa a si todas las entidades son válidas, porque tenemos un patrón de conducta que se autovalida, y si ustedes pueden utilizar información de ese tipo y capacidades analíticas de ese tipo, el tomar algunos de los problemas y resolverlos nos permite enfocarnos en las acciones únicas que requieren más atención y más validación compleja.

Y el flujo es que tenemos que entender, el destruir esas capacidades para entender cuál es la transacción, se tiene, cómo podemos validar la identidad y cómo podemos tener un plan para mandarles un mensaje a los clientes y de hecho, un evento así sucedió en la vida real.

Entonces, la capacitación y la resiliencia son la manera de parar la criminalidad. Y yo sé que hay muchas preguntas y espero responderlas. Con esto quisiera yo cerrar.

- MAESTRA DE CEREMONIAS: Muchísimas gracias, señor Chertoff, Michael Chertoff.

Manuel Romo, moderará esta sesión.

- MANUEL ROMO: Michael es un gran placer tenerte con nosotros y, en particular, alguien como tú, con tu experiencia, con tu trayectoria, estoy seguro que atrae muchísimas preguntas.
Voy a empezar a agruparlas.

Entonces, permíteme empezar con, cómo vamos a tener una conexión desde el punto de vista regulatorio, cómo conectamos lo digital, cómo se vuelve más ágil, cómo podemos aumentar los servicios que ya proporcionamos a través de medios digitales, de banca móvil y a los clientes, y al mismo tiempo tener una regulación que protege en cuanto a los ciber; cómo podemos lograr este equilibrio.

- HON. MICHAEL CHERTOFF: En primer lugar, estoy totalmente de acuerdo. Al ser digitales, un banco nadie es atendida, áreas que tenemos que asegurar a la gente, por medio de la confianza que sus datos van a estar seguros, van a estar disponibles, que nuestras acciones van a ser confidenciales y que no van a estar corrompidas.

Entonces, el rol del Gobierno no es obligar o prescribir maneras de hacerlo, porque francamente pienso que el sector privado es mejor que el Gobierno en cuanto a la mecánica.

Entonces, sin embargo, yo creo que lo que puede hacer el Gobierno es establecer las normas y los requerimientos. Y aquí tenemos las cosas que tenemos que poder demostrar y hacer para cumplir con estos roles.

¿Cómo lo hacemos? Es tu decisión, pero vamos a auditarte y validar que tú tengas seguridad, ya sea que lo hagamos teniendo un equipo que te penetre o tratando a otros que vean tu configuración o para mí la respuesta, esto es lo que tiene que lograr, pero cómo lo haces, esa es tu decisión.

Y ahora quiero relacionar esa pregunta a tu comentario, tus comentarios anteriores, y si entendí correctamente, estábamos hablando de un cambio en la estrategia.

Ya no nos estamos ocupando del perímetro, sino estamos hablando de una protección abierta.

Y cuando nosotros pensamos en un ecosistema impactado, el sistema financiero, los pagos, todo esto abre y cada vez es más extenso. Y en ese sentido podemos proporcionar un comentario de cómo debemos de ver este punto para tener una iniciativa de ciberseguridad en el país.

¿Quién es el jugador, cómo podemos verlo, cuál es la comunicación que existe de nueva vez para implementar una iniciativa de ciberseguridad segura en México? Y como les dije, este tiene que ser un esfuerzo de cooperación, de equipo.

Lo que puede hacer el gobierno a través de regulación directa o del sistema de obligaciones es crear un incentivo positivo y negativo para construir la ciberseguridad en el sistema bancario.

Positivo y negativo porque tenemos que establecer ciertas normas. Si las cumplimos eso se vuelve esencialmente una póliza de seguro contra que te demanden o contra de que te sancione el regulador.

Pero si tu ciberseguridad no es correcta y hay un ataque muy importante, esto se vuelve algo que resulta en un tipo de obligación.

Entonces, la clave más importante es cómo llegamos a un acuerdo para saber cuáles son las cosas que tenemos que lograr para cumplir con las normas, para es seguro desde el punto de vista razonable.

Razonable porque la perfección no es posible. Pero en lo que tenemos que pensar ahí realmente es qué, de nuevo, es práctico en cuanto al a naturaleza del negocio bancario.

Tenemos que ser abiertos a muchos clientes y estamos haciendo banca digital. De hecho, no podemos tener una planta nuclear y nos vamos a desconectar del internet, pero al mismo tiempo tenemos que ver cuáles son las cosas clave que

tenemos que proteger y cómo podemos configurar un servicio o sistema para elevar la protección para estas cosas.

Tenemos algo más en Estados Unidos que se llama la Ley de Seguridad, después de los ataques terroristas de septiembre 11, que quieren decir que, si creas un proceso, una tecnología que es útil para contra terrorismo, que te defiende contra un ataque terrorista y que cumple con unos estándares de calidad.

Entonces, de hecho, te da protección contra las obligaciones y de alguna manera previene que ocurra un ataque. Entonces, el gobierno te tiene que dar la zanahoria y el palo.

Desde el punto de vista bancario es crítico, porque tenemos que estar de la mano, el gobierno tiene que entender la dinámica de la banca para apreciar las medidas de seguridad requeridas, por un lado, pero el sector bancario tiene que tener las perspectivas profundas del gobierno para que nos apoye en cuanto a la conducta de los criminales y para poder trabajar de la mano.

La competencia, la competencia con nuevos entrantes o nuevas personas que entran a los mercados financieros es enorme, entonces no sólo los bancos, no sólo los Fintech, pero los amazons y los googles de ese mundo que proporcionan gran experiencia que la gente entra a sus sistemas, porque son sencillos.

Nosotros como bancos tenemos mucho trabajo para ofrecer el mismo servicio a estos clientes y estos clientes lo están demandando, entonces regresamos a, por ejemplo, la regulación de la prevención contra el lavado de dinero, de conocer a tu cliente, y nosotros mantenemos y seguimos pensando nuevas maneras, si pudiéramos o no hacer, cumplir con los requerimientos de AML y KYC, o sea “ven y conoce a tu cliente y previsión contra el lavado de dinero”, para abrir una cuenta Amazon te permite hacerlo con dos clicks.

¿Cómo lo vemos, cómo podemos luchar con esto? Bueno, aquí hay un área donde lo digital es un beneficio, pero también nos tenemos que preocupar por la seguridad.

Yo creo que mientras más hagamos en línea, mientras más herramientas estén disponibles para cumplir contra el lavado de dinero y conocer a tu cliente mejor, porque en particular el *machine learning* e inteligencia artificial puede haber una

enorme cantidad de transacciones y puede analizar patrones que los seres humanos no notarían a menos que les llamen la atención a ellos.

Entonces, mucho de lo que podemos hacer, desde el punto de vista de inteligencia, de clientes, que estén haciendo algo a un lado, que no esté bien o de conductas contra el lavado de dinero, es más accesible si nosotros pudiéramos verlo a través de los lentes de conducta digital.

¿Y qué viene con ello? Vamos a acumular más datos de lo que hace la gente con su dinero. Eso quiere decir que su privacidad está en riesgo cada vez más y más, y tenemos que asegurarles que estamos protegiendo sus datos y que nadie va a venir a robar sus datos y vamos a explorarlos.

Entonces, al construir esa herramienta analítica para ayudarnos contra el lavado de dinero y conozco a su cliente. Tenemos que hacer cosas para proteger los datos.

Y quisiera yo agregar que también vamos a ver que al obtener inteligencia, por ejemplo, inteligencia de clientes, nos va a ayudar a aumentar la ciberseguridad, porque nos va a hablar de la vulnerabilidad y la actividad maliciosa que a lo mejor tenemos que resolver; o sea, que para mí si se implementa adecuadamente, si una situación en la que todos ganan tanto contra la corrupción y con la ciberseguridad, ambos se resuelven.

Ahora hablemos del eslabón más débil en el ecosistema.

Nosotros vamos a tener una lucha entre los sistemas viejos, antiguos y los APIs, cómo poder mostrar nuevas herramientas al mercado. ¿Usted nos puede dar su opinión sobre cómo desarrollar o tercerizar a proveedores que son terceros? ¿Existe alguna amenaza con lo que se le llama *outsourcing* o tercerización?

Bueno, entiendo porque muchas instituciones bancarias y aquellas que no son tan grandes no tienen las capacidades para desarrollar herramientas que pudieran usarse nuevas capacidades, nuevos *software* para las prácticas bancarias.
Entonces, tenemos que hacernos la siguiente pregunta: ¿podemos asegurarnos que la gente que está haciendo este trabajo, uno, son competentes, y dos, lo que es seguro, lo que usan para poder desarrollar el *software* que están metiendo en su sistema?

De alguna manera un evento que sucedió que fue terrible es RCA, fue una compañía que inventó y mantuvo los tokens usados para darte acceso a ciertas redes como un dispositivo de seguridad y los hackearon, y se robaron el *software* y comprometieron esos token.

Entonces, no estoy seguro que tengamos una opción en términos del *outsourcing* porque la mayoría de los bancos no van a tener la capacidad de desarrollar las herramientas que requerimos para ofrecer nuevos tipos de capacidades.

- MANUEL ROMO: Entonces, déjenme hacer un par de preguntas aquí y vamos a cambiar un poco el tema y vamos a aprovechar su experiencia, lo que ha vivido y el hecho de que esté usted aquí: el virus, el coronavirus.

¿Tiene algún comentario sobre cómo prepararnos, sobre cuál es el estado, cuál es la situación, su punto de vista del mundo? ¿Puede darnos un par de comentarios al respecto?

- HON. MICHAEL CHERTOFF: Gracias por la pregunta.

Quiero empezar diciendo que a lo mejor voy a hacer una observación chistosa, pero hay una razón por la que usamos la palabra virus en el campo de la salud y cibernético, porque las amenazas cibernéticas y las amenazas a la salud comparten el mismo tiempo de modelo.

No viene de una manera en un canal predecible, si no entran estos virus y se distribuyen enormemente. Y hay muchos puntos de entrada y hay muchas maneras de poderlos transmitir y por ello, crean un reto para combatir esta amenaza. Seguimos hablando con un cibervirus que puede venir de diferentes fuentes, o un virus físico o donde, lo que descubrimos es que los retos no sólo hablan de crear la arquitectura, pero de entrenar a la gente sobre cómo comportarse, esto afecta la conducta masiva porque tiene un efecto enorme en nuestra vulnerabilidad.

Muchas veces queremos cerrar la frontera para limitar el coronavirus, tampoco sirvió en el ciberespacio. Esas son comparaciones interesantes, aunque Trump trató de cerrar la frontera. Yo sé que estamos preparados para trabajar con esta pandemia y resolverla y el problema es que hay un alto costo para responder.

Pero el costo más alto es si no respondemos, la respuesta es cierre de eventos grandes, como este. O por ejemplo, dile a la gente que trabaje desde casa, que

los niños no vayan a la escuela. Pero, por otro lado, si no hacemos esas cosas, lo que sucede es que el virus se expone, cada vez más y más gente se infecta y esto resulta en más complicaciones serias para esas personas.

Pero por otro lado estamos equilibrando, porque por un lado no queremos entrar en pánico y cerrar la economía tan rápidamente, pero al mismo tiempo, si esperamos hasta que es claro que tenemos un problema, entonces en ese momento ya estamos proyectando y va a ser muy difícil desacelerar esa proyección del contagio del virus.

Entonces, en el punto en el que detenemos su admisión de la comunidad, o sea que la persona que tiene el virus no sólo voló de Wuhan de donde lo obtuvo, pero más bien es gente dentro de la comunidad que se contagia unos de otros, y en ese momento tenemos que empezar con cambios muy serios en el distanciamiento social, cerrar eventos masivos, a la mejor cerrar escuelas, a la mejor pedirle a gente que trabaje en casa.

Ahora no tenemos que ir tan lejos, pero tenemos que prepararnos y hacer las preguntas, y estoy hablando con los bancos. Si tú vas a ayudar a la gente a trabajar desde casa, tienen las herramientas que requieren, tienen la conectividad, y tienen laptops y desde el punto de vista de la ciberseguridad, hay herramientas, las herramientas son seguras.

Mucha gente si tiene que entrar con la computadora de casa, va a entrar a tu red de banco con un dispositivo infectado, entonces tenemos que asegurarnos que antes de mandar a todos para trabajar en casa, que nos sintamos a gusto, que se conecten de tal manera que sea segura.

Entonces, si hay una cosa que hemos mencionado en esta charla es la preparación y la planeación, porque ahí descubrimos las capacidades que tenemos que acumular y distribuir para estar listos para estas actividades.

Cuando nosotros hablamos del estar listos, cuando hablamos de estos umbrales, de cuándo empezar a actuar de manera, con medidas más radicales, cuánto consenso, cuánta comunicación, cómo resolvemos estos umbrales, cómo los volvemos de conocimiento público en todo el mundo.

Entonces, creo que este es uno de los grandes retos cuando hablamos de las crisis, que es la comunicación.

¿Por qué? Porque cuando nosotros tenemos algo así, cuando estamos infectando el comportamiento masivo, no solo diciéndole a la policía, sino que todos tienen que jugar una parte.

La gente tiene que confiar en ti, tiene que tener claridad, de cuáles son tus expectativas y tienen que entender qué es lo que tienen que hacer. Entonces, la comunicación se vuelve un elemento crítico.

Y yo he visto que las autoridades de salud son las más hábiles para hacer eso. Ellos no necesariamente están equivocados, pero si no minimizan algo que es muy serio, uno de los mensajes que mandaron es que esto se va a difundir y nosotros estamos más allá del punto en donde podemos decir, podemos detener y se va a desaparecer.

Ahora la pregunta es cómo podemos, qué tan serio va a ser. ¿Podemos desacelerar esa difusión? Mientras más la desaceleramos, entonces el sistema de salud va a poder manejar los retos y va a poder ver las medicinas.

Entonces, la clave es que vamos a tener; tenemos que ver cuál es esta amenaza, entonces tenemos que tener un sentido de seguridad y tiene que ser una instrucción clara de qué hacer.

Entonces, la gente va a necesitar evitar cualquier contacto social masivo.

Entonces, yo no sé si el que la gente, yo no creo que la gente esté diciendo que si estás infectado te tienes que quedar en casa, pero si hay eventos de entretenimiento grandes, si están cerrando los teatros en Broadway, realmente muchos de los eventos se tienen que posponer y de la misma manera para muchas personas tienen que trabajar desde casa, si fuera posible, y las escuelas van a tener que cerrar, y también tenemos que tener un paro para aquella gente que no puede trabajar desde casa, entonces tiene que tener un fondo de ingresos.

Si la gente no puede comer van a acabar yendo a trabajar, y eso no va a permitir que cumplamos con este trabajo de tratar de evitar el contagio.

Ahora, quiero hablar de una de las crisis que podemos recordar. Septiembre 11, el tener ese reto y encontrar una solución que realmente cambió la manera como vemos la seguridad en todo el mundo.

Entonces, ¿cómo, cuán paralela es esta coronavirus o esa difusión o esa pandemia del coronavirus contra lo que pasó el 11 de septiembre? ¿Qué lecciones podemos aprender, qué paralelos podemos ser? No es paralelo, porque el 11 septiembre fuimos a Afganistán, invadimos y matamos a Bin Laden, y la razón por la que Bin Laden es diferente del coronavirus es porque puedes matar a individuos o virus individuales cuando atacan tu cuerpo, pero no hay dónde irlos a atacar para matarlos.

El 11 de septiembre requirió un cambio de conducta pública, requirió que fuéramos mejores para obtener inteligencia e información inteligente y también que la gente se adaptara en ciertas conductas para minimizar las amenazas; es decir, seguridad antes de subir al avión o reportar si algo es cuestionable o amenazante, y las autoridades tuvieron que entrenarse para responder rápidamente.

Estos elementos son muy similares al coronavirus, y lo que es más retador cuando vemos esos temas de gobierno, cuando estamos hablando de una crisis o un problema, es un hecho que tenemos que tener conducta pública para cambiar. Una cosa es decirle a la gente en tu gobierno: estás acostumbrado a ser a), ahora tienes que ser b), porque esa gente sigue órdenes.

Pero cuando tienes miles de millones de personas que se conduzcan y comporten de manera distinta y tenemos diferentes niveles de compromiso y de comprensión, es difícil de lograr, por ello es diseñar un programa y un plan que sea claro, accesible y práctico; es algo que está en el corazón contra el terrorismo en septiembre 11 y está en el corazón de manejar las pandemias.

Y por eso cuando estuve en DHS hicimos escenarios de planeación para ataques terroristas, entonces en la misma sesión de planeación también vimos qué hacemos con una epidemia o pandemia importante cuando estábamos preocupados del bioterrorismo.

Y en ese sentido creo que la práctica de subirse a un avión debido a la seguridad ha cambiado. Y en este momento es algo que es natural de lograr.

- MANUEL ROMO: ¿Cuáles son tus expectativas en cuanto a este virus? ¿Cómo va a cambiar la vida diaria?

- HON. MICHAEL CHERTOFF: Creo que durante un rato muchos de los eventos públicos se van a posponer o se van a cancelar.

Lo que están tratando de hacer es desarrollar tres cosas: la primera es una prueba rápida, si tenemos o no el virus; por ejemplo, Singapur, cuando hay una epidemia o una pandemia tan pronto llegas al aeropuerto ellos tienen a alguien que te escanea si tienes fiebre o alguna señal de lo que les preocupa. La prueba tiene que acelerarse.

En segundo lugar, una vacuna, en segundo lugar porque esa es la mejor solución.

Y en tercer lugar vamos a derrotar, pero por ejemplo, con el flu estos virus mutan, entonces siempre hay un atraso de la vacuna y paliativos, cosas que podemos sumar para reducir los efectos, aunque no vacunemos a las personas estos son tres frentes en donde vemos acción, y una de las grandes incógnitas es la siguiente.

Es esto de temporada como el flu o la gripa, si es de temporada entonces no se va; si el clima es más cálido, entonces de alguna manera podemos ver y trabajar para prepararnos más, para combatir el virus en lo que llega el siguiente invierno.

- MANUEL ROMO: Cooperación internacional escuchamos y entendemos que hay iniciativas para estar más aislados, que los países se aíslen, y en ese sentido cuando un virus entra y ataca, entonces golpea a todos realmente.

De cooperación internacional no sólo aislar a un país y la excepción de un país es una cosa, pero realmente cooperación internacional, ¿cómo ve usted el ambiente para hacerlo entre las entidades públicas, políticas y privadas?

- HON. MICHAEL CHERTOFF: Esa es una pregunta difícil. Vivimos en una era en donde todos estamos hablando del nacionalismo en donde mi país primero.

Y la ironía es que en el mundo moderno algunas de las amenazas no, cuando estamos en la era del cambio climático, pandemias globales, nadie puede hacerlo solo.

Si mi actitud es: “yo voy a hacerlo, y yo gano y tú pierdes”. Es un juego en donde todos perdemos, porque estamos hablando de lo que se llama el problema global. Es algo que como el aire y el agua circulan en todo el mundo.

Entonces, si una persona no juega de acuerdo con las reglas y puede afectar el ambiente de manera adversa y todos los demás sufren, pero también ellos porque no podemos cerrarnos y aislarnos. El virus nos está enseñando una lección y la lección es: “no puedes hacerlo todo”.

Estas son de las amenazas más serias que enfrentamos y al hacer lo mejor por nuestras ciudades quiere decir: cooperar con otros países, no tratar de una u otra manera aprovecharse de lo mismo con la ciber-amenaza.

Sí, la verdad es que tenemos hacer revertir la globalización. La única manera es eliminar el agua y el aire, y el Internet. Y ninguna de esas cosas van a suceder. No podemos eliminar la globalización.

- MANUEL ROMO: Michael, muchas gracias por tu tiempo y por estar aquí.

- MAESTRA DE CEREMONIAS: Muchísimas gracias, señor Chertoff por su tiempo.

Agradecemos al licenciado Romo por su presencia en el escenario.

Procederemos al primer receso de las actividades de hoy, mismas que se reanudarán en punto de las 11:20 a.m.

Les pedimos por favor, contar con su puntualidad para comenzar con tiempo con la conferencia.

La Asociación de Bancos de México agradece su asistencia.

- - -o0o- - -