

# RELATORÍA

Ciudad de México, 28 de marzo de 2018

## “CAPITAL SINNIX: Innovación y Ciberseguridad”



Imagen del Centro de Estudios Internacionales Gilberto Bosques

*El 12 de marzo de 2018, la Organización de los Estados Americanos junto con Propulsar, la Asociación Mexicana de Internet y otras organizaciones públicas y privadas auspiciaron un día de discusión acerca de la ciberseguridad en el mundo. El día fue parte de la semana de innovación social CAPITAL SINNIX, durante la cual se habló de innovación, tecnología y emprendimiento, entre otros temas con miembros del sector público, privado, académico y la sociedad civil.*

## Introducción – Conferencia Magistral de Claudio X. González

El 12 de marzo en el Hotel *Four Seasons* de la Ciudad de México, inició el primer día de CAPITAL SINNIX. Esta cumbre dedicada a la innovación tecnológica buscó generar un diálogo entre agentes gubernamentales, académicos y empresarios latinoamericanos con el propósito de encontrar soluciones a problemas globales y comunes mediante el uso de la innovación social.

El evento comenzó con la transmisión de un mensaje previamente grabado por el Secretario General de la Organización de los Estados Americanos (OEA) quien insistió en la importancia de impulsar el desarrollo tecnológico, la innovación y la cooperación para la ciberseguridad para el bien de América Latina. El Secretario aseguró que la tecnología ha logrado democratizar muchos espacios y acercar a miles de personas, pero también ha servido para incrementar la desigualdad y la marginalización de muchas personas que no tienen acceso a la misma. Por ende, buscar desarrollar tecnologías incluyentes y en el beneficio de todos, así como continuar enfrentando los nuevos retos que dichas tecnologías suponen como meta de todos los Estados.

A continuación, se dio inicio a la ponencia del conferencista magistral, Claudio X. González, quien habló desde su experiencia como servidor público, activista social y abogado. Su presentación fue desde su posición como Co-fundador y Presidente de Mexicanos Contra la Corrupción, organización ciudadana que busca combatir la corrupción y la impunidad a través de “la exigencia de cambio y propuesta de mejora”. González comenzó hablando de la importancia de la innovación social como herramienta para resolver dos enormes problemas en América Latina: la falta de educación de calidad y de estado de Derecho. Subrayó que en el país no se aplican las leyes por igual y la ley que importa “es la del más poderoso”. México ocupa el lugar 130 de 170 en el índice de percepciones de transparencia internacional, lo cual lastima las inversiones extranjeras y por ende hace que perdamos competitividad. La inseguridad personal y patrimonial en los negocios “asusta” capitales extranjeros, por lo cual la corrupción tiene un efecto grave y significativo en el crecimiento del país.

El ponente estima que la corrupción cuesta alrededor del 5% del PIB anual (900 mil millones de pesos), más está es una estimación conservadora que podría incrementarse mucho más dependiendo de las consideraciones con las cuales se calcule. Asimismo, considera que la corrupción genera un daño, que además de lastimar a las instituciones, la confianza pública y las operaciones del Estado, le cuesta al ciudadano un impuesto regresivo de entre el 14% y 30%. Esto, dado que miles de millones de pesos desaparecen de programas destinados para servicios básicos como infraestructura o seguridad y que, por ende, las personas tienen que utilizar sus propios recursos para solventar los espacios que no logra llenar el Estado. Asimismo, todas las compañías que deben de pagar sobornos y extorsiones. para operar en México, elevan el costo de los productos, costo que acaban solventando los consumidores.

No obstante, la corrupción es un fenómeno privado y social, no exclusivamente público. “La iniciativa privada en México se comporta muy mal”, aseguró González al destacar que también los ciudadanos participan en actividades de corrupción. La impunidad en México en 2015 fue del 97% - cifra alarmante que evidencia la extensión de éste fenómeno. La corrupción está frenando el desarrollo económico, incrementando la violencia e inseguridad, exacerbando la desigualdad y socavando a las instituciones públicas. Acabar con esto requiere la capacidad de innovar desde la sociedad. Es la sociedad organizada y atrevida quien hace que funcione el aparato gubernamental.

Mexicanos Contra la Corrupción es un “*think tank*” y “*do thank*” innovador porque utiliza la investigación aplicada, investigación periodística, litigio estratégico, comunicación y movilización social desde la “trincheras ciudadana”. Hasta ahora, destaca que no existe otra organización en América Latina que opere de la misma forma. No es solamente un espacio crítico, pero es un espacio propositivo que estudia, diagnostica, exige y propone maneras de hacer de México un país más transparente y donde opere la ley. El Sistema Anticorrupción,

que califica González de “barroco” es un resultado de esfuerzos ciudadanos en respuesta a la corrupción desde el Ejecutivo en el caso de la “Casa Blanca”. El ponente destaca que México tampoco cuenta con una fiscalía independiente, a diferencia de otros países latinoamericanos que han sido mucho más activos en los casos de *Odebrecht* u otros tipos de corrupción en altos niveles.

Parte del trabajo de Mexicanos Contra la Corrupción, afirmó, tiene que ver con investigaciones que revelaron las empresas fantasmas y las redes de corrupción del ex Gobernador de Veracruz Javier Duarte, así como otras operaciones de lavado de dinero operado desde el nivel Federal. Duarte “financió masivamente la campaña del actual Presidente de la República”, por lo cual el Ejecutivo “no quería” actuar en su contra, pero el nivel de indignación y el escándalo mediático que generaron las investigaciones, causaron, a criterio de González, que tuviesen que actuar en su contra. Aunque no ha sido un sistema perfecto y el ex funcionario aún no recibe castigo, el ponente considera que es un avance en términos de la aplicación de la justicia en México. He aquí donde se muestra la efectividad de la presión ciudadana y mediática.

El hecho de que la corrupción sea un fenómeno tan común hace que la denuncia sea un gran riesgo, a lo cual González argumenta que entre más personas denuncien y participen, menos será el riesgo al que se enfrenten. La lógica inversa es la actual: en donde solamente unos pocos se atreven a levantar la voz y por ende corren enormes riesgos. Parte de mitigar este riesgo ha sido el uso de redes sociales que permiten distribuir la información de manera democrática, pero es solamente una de las aplicaciones positivas de estos avances.

Finalmente, el Presidente de Mexicanos Contra la Corrupción aprovechó para decir que la tecnología y la información tecnológica eliminarán trabas burocráticas y consideraciones absurdas, utilizando *Big Data* para investigar corrupción, abrir canales de denuncia pública anónima, difundir investigaciones y litigios, y coordinar a la sociedad civil organizada. El sistema fiscalizado electrónico también es útil para hacer del país uno más transparente, aunque hay que “cuidar” la manera en la cual se usa este sistema. Cambiar las cosas en México y Latinoamérica, en materia educativa, de salud y de seguridad conllevará muchos riesgos, pero éstos deben asumirse ya que el riesgo más grande es “no atreverse”.

### **Estrategias de ciberseguridad: retos y desafíos**

El primer panel comenzó con la participación de la Mtra. Bárbara Marchiori, representante del Programa de Ciberseguridad de la Organización de los Estados Americanos. La Mtra. Marchiori habló de la necesidad de crear estrategias de ciberseguridad en el plano nacional y emitió algunas recomendaciones para el diseño e implementación de las mismas. En este sentido, mencionó que se debe reunir la mayor cantidad de esfuerzos, involucrando al sector privado y público. Afirmó que la identificación de amenazas y riesgos, así como consultas y mecanismos de participación precisarán el diseño, teniendo como resultado una estrategia efectiva. Aunado a lo anterior, hizo énfasis en el papel del legislativo y el presupuesto en la implementación. Por otro lado, en el caso específico del papel de la OEA, enumeró ocho casos de estrategias de ciberseguridad dentro de la organización y presentó otros tres que son diseñados actualmente en colaboración Estado-OEA.

En contraste, el Dr. Jorge Cerdio, decano de la Facultad de Derecho del Instituto Tecnológico Autónomo de México, tituló su ponencia “Innovación, regulación y educación pública”, argumentando que abordaría una perspectiva del sector académico y de educación. La tesis en la que estuvo basada su argumentación es que, debido a que la forma de hacer negocios y las transacciones jurídicas estarán altamente impactadas por el desarrollo tecnológico, se requieren individuos capaces de enlazar lo que llamó “puntos de contacto” entre el problema, la solución y los datos producidos.

Aunado a lo anterior, mencionó que esto supone un doble reto. En primer lugar, en materia de seguridad, se requiere evitar que terceros puedan interferir en la producción y la operación de estos nuevos modos de realizar transacciones jurídicas y comerciales. En segundo lugar, considerado por el ponente como el más importante,

dijo que es necesario prepararse y reaccionar para generar y aprovechar el capital humano específico y así generar una regulación adecuada. En este sentido, expresó que sin una adecuada regulación a aquellos profesionistas que están encargados de la innovación, esta puede simplemente no prosperar y defendió que la única forma de crear individuos capaces es la educación.

El Dr. Gabriel Juárez, Viceministro de Tecnologías de la información y Comunicación de Guatemala, narró lo que, a su perspectiva, son los retos, las amenazas, oportunidades, necesidades y éxitos en materia de ciberseguridad. Dijo que América Latina enfrenta retos como la creciente inclusión de nuevas tecnologías cibernéticas en temas como narcotráfico, tráfico de armas, crimen organizado internacional e incluso terrorismo. Desde otro punto, afirmó que existen dos principales retos que su país afronta en la materia: garantizar la seguridad en la utilización de las redes sociales y regular las redes sociales, defendiendo la libertad de expresión, la participación equitativa y la inclusión en las nuevas tecnologías.

Aseguró que ningún país ha resuelto estos retos, pero el Gobierno guatemalteco brinda su mejor esfuerzo y ha obtenido varios logros en esta materia. Para sostener esto, presentó un estudio de la Organización de los Estados Americanos (OEA) que divide a los países de acuerdo con el nivel de madurez en materia de ciberseguridad, mostrando que ninguno supera el nivel 2, lo que significa que no poseen o poseían la capacidad de crear instrumentos jurídicos, políticos y educativos para combatir la ciber inseguridad. Por otro lado, afirmó que la formación del Consejo Nacional de Ciberseguridad Mexicano abrió paso para trabajar de manera interinstitucional y generó resultados positivos. Por último, presentó algunos de los proyectos en los que trabaja como la Ley de Ciberdelincuencia y la Nueva Estrategia de Ciberseguridad. Concluyó que es necesaria la participación conjunta de todos los involucrados para el éxito y diseño de nuevos marcos de ciberseguridad.

### **Una llamada a la acción para proteger a ciudadanos, sector privado y gobiernos**

El segundo panel comenzó con la participación del Mtro. Victor Lagunes, jefe de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República de México. El Mtro. Lagunes dirigió su ponencia en los siguientes rubros: innovación social, gobernanza, dinámicas para la creación de política pública, estrategias y prevención al ataque cibernético público y privado. Afirmó que el mayor reto de ciberseguridad nacional es acercar a los funcionarios a las innovaciones de las universidades y hubs de manera acertada, para responder a los retos creados por el riesgo de la conectividad.

De esta forma, dijo que con la construcción de una política de ciberseguridad robusta llega una preocupación muy grande en materia de Derechos Humanos, por lo que concluyó que la estrategia federal no es “el gobierno tratando de decidir qué es mejor para los ciudadanos” sino crear un entorno responsable donde cada individuo desde su lugar delinee una estrategia para prevenir la inseguridad cibernética.

En contraste, el Mtro. Miguel Rego, socio de *iHackLabs LTD*<sup>1</sup> habló principalmente del texto académico que elaboró para la OEA titulado “un llamado a la acción para proteger a ciudadanos, sector privado y gobierno”, haciendo especial énfasis en que el desarrollo de la vida digital no solo es una cuestión de protección al riesgo y la amenaza, sino de oportunidades para los tres entornos que aborda en su artículo.

En primera instancia, dijo que el desarrollo tecnológico es una buena oportunidad para las empresas y los jóvenes, debido a que es un mercado altamente demandante que requiere de profesionales, siendo este un campo perfecto para el emprendimiento y el desarrollo. Afirmó que lo anterior llevaría a no depender de soluciones de otros países, logrando así un enfoque de Estado. En consecuencia, mencionó que el gobierno debe ser un facilitador o acelerador, pero que la ciberseguridad depende de todos, incluyendo el sector privado.

---

<sup>1</sup> Compañía internacional de ciberseguridad.

Concluyó que la innovación es importante y para llegar a ella se requiere del esfuerzo científico, académico, político y empresarial.

Por último, la Mtra. Abby Daniell, gerente de Desarrollo Comercial para América Latina, Canadá y el Caribe de Amazon habló sobre *Amazon Web Services*<sup>2</sup>. Comenzó su ponencia reiterando la alianza estratégica que existe entre la institución y el concepto de ciberseguridad. Mencionó que la principal función de *Amazon Web Services* es entregar productos, servicios y contenido de empresas, particulares, gobiernos e instituciones sin fines de lucro, siendo esta empresa un claro ejemplo del uso de la tecnología en el sector privado. Posteriormente, narró la historia de *Amazon Web Services* y comunicó que a sus 12 años y con más de un millón de clientes, es la empresa de Tecnologías de la Información (TI) más grande del mundo.

De forma consecutiva, dijo que “la nube”, una de las principales herramientas de *Amazon*, es la fundación para muchas tecnologías emergentes como inteligencia artificial e Internet de las Cosas debido que facilita la innovación. En este sentido y con relación al panel, dijo que la nube es una herramienta importante para mejorar a una organización porque conlleva mayor seguridad de cada caja e infraestructura y afirmó que, comparada con la infraestructura tradicional, la nube fortalece la postura de ciberseguridad en una organización. Por último, pidió el apoyo del sector público para lograr mejores resultados y mencionó algunos mecanismos que la empresa posee para apoyar en el desarrollo de las estrategias nacionales de ciberseguridad.

### **Innovación y ciberseguridad desde el sector privado**

Eduardo Palacios López, representante de la Unidad de Seguridad de IBM, abrió el tercer panel estableciendo la importancia de extrapolar el entendimiento de ciberseguridad como concepto a audiencias no técnicas con el fin de que éstas ayuden a gestar un nuevo paradigma para el sector privado en donde no solo se abarquen aspectos tradicionales, sino aspectos como identidades, acceso de datos, aplicaciones de infraestructura, etc. El cambio de paradigma fungió como el núcleo de la primera ponencia en la cual se enfatizó la necesidad de cambios en aspectos de procesos, estándares e incluso reclutamiento, partiendo del punto de la falta de interés de los estudiantes por temas de seguridad. Finalmente, tocó el tema de género en donde presentó datos que muestran que sólo 10% de los puestos vinculados a la seguridad los poseen mujeres, haciendo explícita la necesidad de cambiar la forma en la que se habla de seguridad.

Como segunda ponencia, el gerente de certificación de tecnologías de la información en *NYCE*<sup>3</sup>, Pablo Corona Fraga, comenzó exponiendo el vínculo entre la percepción de ciberseguridad con el miedo, por su parte, propuso desligar ambos conceptos por medio del entendimiento del primero así como de su cercanía con la gente a través de su superficie de contacto que aumenta más cada vez mediante dispositivos cotidianos que a su vez están conectados a internet. El problema con lo anterior radica en que debido a las diferentes prerrogativas que éstos tienen, la prioridad de su red debe ser distinta, cosa que no sucede.

Finalmente estableció que la mayoría de las organizaciones piensan que están preparadas para los ataques cibernéticos cuando no es así, dado que existen creencias equivocadas en donde la seguridad se percibe como un actor estático. Otro error que señala es la certidumbre de que la ciberseguridad únicamente se asocia al *hardware* y *software* cuando en muchos casos se trata de errores humanos. Corona Fraga terminó su exposición dando pie a la creación de soluciones pro-activas con fuertes componentes de innovación y

---

<sup>2</sup> Rama de la compañía Amazon cuya plataforma es ampliamente conocida como espacio de compra por internet. *Amazon Web Services* se encarga de atender necesidades específicas de empresas mediante el uso de tecnología avanzada, por lo cual es una plataforma distinta.

<sup>3</sup> Organismo de Certificación de Producto de la Industria Electrónica, Industria Hulera, Unidad de Verificación de Información Comercial y como Auxiliar en el Control Sanitario de Medicamentos y Dispositivos Médicos.

actualización, además de un entendimiento integral de la tecnología sujeta a procesos, personas, seguridad física, etc.

La tercera ponencia estuvo a cargo del Diputado Vidal Llerenas Morales el cual abordó el tema de la importancia de la interacción entre el sector público y privado con relación a la seguridad informática. Para comenzar, el ponente acentuó la importancia de la cooperación con el fin de tener mayor marco de acción en la generación de legislación con respecto al tópico, como ejemplo, éste compartió con el público su experiencia en el casi inexistente diálogo en la Cámara de Diputados con relación a temas de tecnología, innovación y ciberseguridad debido al poco conocimiento que se tiene sobre los mismos. Como conclusión, advirtió la necesidad de retroalimentación con respecto a los temas mencionados con el fin de ejecutar legislación pertinente y así rescatar beneficios de la innovación tecnológica para su uso en problemas de seguridad nacional, como el combate al crimen organizado. Después, Juan Pablo Castro, director de tecnología y ciberseguridad de *Trend Micro*<sup>4</sup>, abordó la necesidad del entendimiento de la ciberseguridad en audiencias no técnicas, es decir, llevar el concepto a distintas áreas de la sociedad para facilitar el proceso de legislación. Así, enfatiza lo imperativo de la diferenciación entre ciberseguridad y privacidad además de vincular la primera con los procesos de innovación, estableciendo que ambas deben desarrollarse al mismo paso y que son dependientes entre sí debido a que en muchas ocasiones, las vulnerabilidades se centran en un proceso de innovación rápida que muchas veces se efectúa cometiendo errores.

Finalmente, Horacio Martín Contreras de *HUAWEI*<sup>5</sup>, estableció una tesis sobre la cual su ponencia estuvo constituida: “la vulnerabilidad se encuentra en todos lados”, y por lo mismo señaló que es imperativo que exista un sistema de seguridad integral en donde todas las capas estén protegidas. A su vez, se centró en los retos que se presentan con relación a los cambios tecnológicos, tomando en cuenta que el desarrollo desenfrenado de los mismos conlleva a su vez riesgos que las leyes locales no están preparadas para cubrir. Propone percibir el estado de la cuestión como un ecosistema en donde el operador, usuarios, y aplicaciones de industria estén integrados bajo una misma estrategia. Para lo anterior, añadió algunos puntos<sup>6</sup> importantes los cuales están basados en diferentes textos académicos, como la ejecución de análisis, fortalecimiento de la seguridad por medio de identificación de actores, aplicación de políticas y reglas internas, así como la verificación y actualización de estándares diseñados por organismos internacionales.

## La innovación política y la ciberseguridad

El cuarto panel comenzó con Jessica Vera, consejera local del INE en el estado de Nuevo León, la cual hizo dos interrogantes en cuanto al tema central del ciclo de conferencias: ¿Cómo nos podemos involucrar? y ¿Cómo se puede involucrar el gobierno?, ligando ambas con el papel de las empresas de transferencia y confianza en ciudadanía. La ponente afirma que la ciberseguridad representa un tema de gran complejidad en los diferentes estados de la República y de la necesidad de supervisar por medio de esta herramienta las elecciones a través de su cómputo, aterrizando en el espectro distrital en donde existe la mayor actividad ciudadana y en donde se distinguen más áreas de oportunidad debido a la falta de capacitación por parte de los individuos que participan en el ejercicio de supervisión de las elecciones del año en curso.

Por otro lado, señala la importancia de la seguridad informática en las presentes elecciones y su vulnerabilidad a ataques cibernéticos que pueden tener lugar debido al status segregado del INE. Esto implica que existen

<sup>4</sup> Compañía de ciberseguridad y defensa más grande del mundo.

<sup>5</sup> Compañía de tecnología de la telecomunicación.

<sup>6</sup> Seguridad del siglo XXI (2012), 2. ¿Cómo incluirías ciberseguridad en el ADN?, los 100 requerimientos para tener una seguridad integral.

diferentes sistemas que apoyan la organización de las elecciones. El más importante, según la ponente, es el voto en el extranjero en donde existen 570,789 personas de padrón electoral y 184,989 en la lista nominal.

Durante su participación se mencionaron las acciones tomadas por el INE con el fin obtener la confianza ciudadana durante las elecciones: el auto reconocimiento y la estrategia de cultura cívica, entre otros. Finalmente, mencionó que la legitimidad de la institución ha aumentado debido al acercamiento que ésta ha tenido a la población por medio de consejeros generales e interacción a través de redes sociales. Asimismo, la apertura al diálogo ha sido mucho más evidente gracias al apoyo de programas como su Estrategia Nacional de Cultura Cívica y cooperación con la OEA.

Como segundo ponente, Gerardo Pérez Gallardo, miembro de la Alianza para el Gobierno Abierto de la OEA, habló sobre la representación política desde el punto de vista de la innovación social. Como primera instancia, se refirió al problema de representación que se refleja en las cifras de diferentes investigaciones<sup>7</sup> que arrojaron que aproximadamente el 70% de los mexicanos no se sienten representados, aunque por el otro lado, 7 de cada 10 personas creen que participando conjuntamente con el gobierno se pueden disminuir los problemas. Tomando en cuenta lo anterior, el ponente compartió con la audiencia una experiencia en Jalapa, Veracruz, en donde por medio de la cooperación entre ciudadanía, organizaciones civiles y la administración pública se ejecutó un programa en el que se elaboró una aplicación para conocer los recorridos de los camiones de transporte público, así como los tiempos aproximados de trayecto y cercanía. Lo anterior se hizo por medio de la identificación de una problemática concreta y un esfuerzo para su resolución con la ayuda de un diálogo horizontal y la utilización de tecnología. Finalmente, Gerardo Pérez enfatizó que una actitud de transparencia lo era todo para obtener la confianza de los ciudadanos, y así elaborar programas incluyentes y participativos con un uso adecuado de la tecnología para tener más impacto.

Para cerrar el último panel, Clicerio Coello Garcés, quien funge como visitador del Tribunal Electoral del Poder Judicial de la Federación, estableció que el principal problema es el alto índice de desconfianza de la sociedad con respecto a la función política. Para el ponente, se vuelve clara la necesidad de ingenio y talento para tomar acciones con el uso de innovación para el proceso de edificación de confianza. El déficit de la misma, genera una serie de problemas en donde los más significativos son la falta de legitimidad en las autoridades, representación y en las acciones que éstas ejecutan, así como la erosión de puentes fidedignos de comunicación entre la sociedad y su representación y por último su desempeño y la repartición de justicia. Como acción concreta, propone la generación de un modelo de transparencia con el fin de llevar a cabo una acción conjunta con la ciudadanía e instituciones que contribuyan a una nueva repartición de justicia y fortalecimiento institucional.

En el tema de ciberseguridad, estableció la necesidad de apertura el desempeño judicial siempre y cuando este se dé con el debido cuidado con relación a aspectos que deben mantenerse bajo control, éste estableció que se tienen que tomar en cuenta la manera en cómo se publica la información para que la población dé seguimiento a las controversias. Finalmente, dio a conocer los puntos con el que la justicia abierta se manifiesta en un tribunal los cuales son datos abiertos, las sentencias con lenguaje ciudadano, el tema de la accesibilidad e inclusión en la justicia electoral, la transparencia en el desempeño judicial, y por último la interacción con la ciudadanía.

---

<sup>7</sup> Análisis de transparencia internacional y transparencia mexicana.



CENTRO DE ESTUDIOS INTERNACIONALES  
**GILBERTO BOSQUES**  
ANÁLISIS E INVESTIGACIÓN

**Coordinadora General**  
Adriana González Carrillo

**Coordinación y revisión**  
Arturo Magaña Duplancher  
Ana Margarita Martínez Mendoza

**Investigación y elaboración**  
Inés Carrasco Scherer  
Leticia Pérez Navarro (Servicio Social)  
Eugenia Flores (Servicio Social)

**Marzo de 2018**

El **Centro de Estudios Internacionales Gilberto Bosques** del Senado de la República tiene como objeto la realización de estudios y el acopio de información sobre temas de política internacional y política exterior de México; así como el prestar apoyo a las comisiones de relaciones exteriores para el desarrollo de sus actividades y el ejercicio de las facultades exclusivas del Senado en materia de política exterior; además de auxiliar a los órganos directivos, comisiones, grupos parlamentarios y senadores que así lo requieran en cuanto a diplomacia parlamentaria y protocolo en el ámbito internacional.

 **CGBSenado**

<http://centrogilbertobosques.senado.gob.mx/>