LA CIBERSEGURIDAD Y LOS CIBERATAQUES

Departamento de Derecho de las Telecomunicaciones de la Universidad Externado de Colombia

Compilado por:

Ricardo Andrés Esguerra Alzate

Monitor del Departamento de Derecho de las Telecomunicaciones Universidad Externado de Colombia

28 de junio de 2023

Bogotá D.C., Colombia

Calle 12 No. 1-17 Este

Bogotá D.C., Colombia

Teléfono: 282 60 66 Ext. 1105, 1106 esdercom@uexternado.edu.co

Jornada de 8:00 a.m. – 1:00 p.m.

Panel: Política nacional de confianza y seguridad digital. Un balance y cómo avanzar

Moderador: Jorge Fernando Bejarano – Experto en TIC y docente universitario.

Panelistas:

Orlando Palomá – Fiscal Especializado. Dirección Especializada contra Delitos Informáticos

Óscar Salazar – Representante del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT)

Rafael Rodríguez – Director de la Red Nacional Académica de Tecnología Avanzada (RENATA)

Julio César Mancipe – Asesor senior en Seguridad Digital y Ciberseguridad de la Consejería de Transformación Digital de la Presidencia de la República

El moderador preguntó al Dr. Salazar que cuál era su balance sobre las acciones a cargo de MinTIC frente a formación de servidores públicos, temas de información, desarrollo de capacidades.

El ponente inició su discurso mencionando que, desde la perspectiva de las políticas públicas, Colombia tiene muchísimo por ofrecer y alcanzar. Señaló que con el CONPES 3995 se dio un gran salto frente a la potencialización de la seguridad digital en el país, y que desde el Departamento Nacional de Planeación (DNP) ese CONPES se planteó como una necesidad vista desde tres grandes ejes: i. Capacidades de la ciudadanía frente a temas de ciberseguridad y ciberdefensa. Destacó que la ciberdefensa sigue siendo muy relevante en el país, principalmente en las Fuerzas Militares; ii. Gobernanza. Señaló que no existía antes un responsable en materia de ciberseguridad, por lo que se decidió que es la Presidencia de la República quien coordinaría las actividades en materia de seguridad digital del país, de donde surgió un marco de gobernanza frente a la ciberseguridad; iii. Llamado a la actualización normativa. Mencionó que lo relacionado con los planes estratégicos de tecnologías se han impulsado no solo con las políticas de seguridad digital, sino también con las políticas de gobierno digital, en lo que tiene que ver con las competencias de MinTIC para el sector público, donde se hace un llamado para realizar estos planes estratégicos de manera sectorial.

Ahora bien, el Dr. Salazar indicó que COLCERT es una persona jurídica que acude ante la emergencia cibernética a mitigarla, es decir, que es una especie de primer respondiente ante ataques cibernéticos y que se ha acudido a tal grupo tanto desde el sector público como el privado.

El moderador retomó el uso de la palabra, destacando de la exposición del Dr. Salazar que cuando las entidades hallan guías y protocolos a los que pueden acudir gratuitamente en materia de ciberseguridad, tanto en sector público como privado, el sector TIC se fortalece.

Procedió a darle la palabra al Dr. Julio César Mancipe, a quien le preguntó sobre el Decreto 338 de 2022, cuyo aspecto característico es que propuso un esquema de gobernanza de seguridad digital, ordenando su adopción. Preguntó al Dr. Mancipe sobre los planes de la Presidencia de la República frente a la implementación del modelo de gobernanza planteado en el decreto y cómo se articula tal modelo con la creación de la Agencia Nacional de Seguridad Digital.

El Dr. Mancipe comenzó su intervención introduciendo el Decreto 338 de 2022, de donde destacó el Comité Nacional de Seguridad Digital que inició formalmente en 2023. Mencionó que se creó un primer grupo de trabajo, cuyo fin fue acelerar cualquier lineamiento que requiriese el Estado y el sector privado en temas de ciberseguridad, y también tratar lo relacionado con infraestructuras críticas.

Además, resaltó que por la cantidad de ataques que se han presentado, se habilitó un puesto de control coordinado por Presidencia donde interactúan varios agentes para gestionar frente a organizaciones del sector privado las mejores oportunidades para recuperarse de tales ataques. Se refirió aquí a la creación de la Agencia Nacional de Seguridad Digital, quien llegaría, en caso de aprobarse en el Congreso el proyecto de ley, a asumir algunas de las tareas o funciones que se consagran en el Decreto 338 de 2022.

El Dr. Bejarano mencionó frente a la intervención del Dr. Mancipe que el modelo de gobernanza de seguridad digital persigue la generación de espacios que fortalezcan la interacción entre los distintos actores, pasando de un esquema donde primaba la presencia estatal, a uno más abierto y participativo donde ingresan otros agentes (incluso privados) para realizar trabajos conjuntos y armónicos que fortalezcan el sector. Para ello, preguntó que, desde el sector educativo, cómo se puede fortalecer la interacción entre actores para articular las políticas públicas en estos temas.

Tomó la palabra el Dr. Rafael Rodríguez, quien sostuvo que el tema de ciberseguridad es de alto impacto, es un tema disruptivo que debe tratarse de manera contundente y radical. Señaló que la interacción de cuatro actores es fundamental para robustecer el sector de la ciberseguridad en el país: i. Comunidad en general, representada en agremiaciones y otras entidades; ii. Academia, pues es allí donde está el conocimiento, el avance y la innovación; iii. Industria, pues es quien genera la tecnología y el conocimiento frente a la ciberseguridad; iv. Gobierno, a través de una agenda de políticas clara.

Señaló que desde RENATA están desarrollando el clúster dirigido a la educación, ubicando desde las mejores empresas de desarrollo tecnológico en el mundo y preseleccionan 4. Por ejemplo, seleccionaron a Fortiner, que es una empresa muy fuerte, o Check Point. Estas empresas son las que permiten conocer cómo es el statu quo actual de la ciberseguridad y la ciberdefensa.

Concluyó que desde RENATA proponen implementar un mecanismo muy articulado, con diversos sectores de la economía donde interactúen los cuatro actores mencionados, para así ir un paso delante de la ciberdelincuencia y así lograr prevenir y mitigar los ciberataques.

El Dr. Bejarano se refirió a la exposición del anterior ponente y dio un dato muy interesante, pues mencionó que Colombia es el país que mejor tiene arraigado y desarrollado el concepto de clúster en Latinoamérica, pues el país cuenta con más clúster que cualquiera en la región.

Le mencionó al Dr. Palomá sobre las capacidades que está generando su Dirección al interior de la Fiscalía para combatir el flagelo de la ciberdelincuencia.

El ponente destacó que la ciberdelincuencia en el país es alarmante, pues cada día las amenazas digitales y electrónicas aumentan exponencialmente, y que además no son fáciles de llevar al conocimiento de la judicatura. Mencionó que a raíz de todo esto se creó la Dirección Nacional contra los Delitos Informáticos, la cual ha congregado una serie de recursos técnicos y humanos muy especializados para combatir la creciente ciberdelincuencia.

Sostuvo que dicha Dirección conoce de la infraestructura crítica y de cómo protegerla frente a dichos ataques cibernéticos, por lo que ya se han ido identificando “ciberdepredadores” que son grupos que han destinado su actividad a delinquir por la web de manera organizada, sistemática y frecuente. Si bien resaltó varias veces lo difícil que es luchar contra la ciberdelincuencia, mencionó que desde la Dirección Nacional contra los Delitos Informáticos han luchado y lo seguirán haciendo para prevenir, atacar y castigar dichos ataques cibernéticos.

El Dr. Bejarano destacó la gestión que ha tenido la Dirección Nacional contra los Delitos Informáticos hasta ahora, para preguntarle al Dr. Óscar Salazar sobre los planteamientos del CONCERT frente a la visión del nuevo gobierno para fortalecer la ciberseguridad del país.

Respondió el Dr. Salazar que, si bien es un grupo pequeño, el CONCERT ha trabajado arduamente para fortalecer la ciberseguridad nacional. Destacó que un aspecto fundamental es la seguridad de operaciones, tema en el cual el país está aún muy replegado.

Se refirió al fortalecimiento de las capacidades desde MinTIC y los enfoques que se han tomado para conseguir tal fin: un enfoque en educación, el cual cubre y aprovecha la capacitación del SENA, quien brinda en una de sus líneas de enseñanza la ciberseguridad, haciendo énfasis en los servidores públicos. Otro elemento propuesto por el Ministro TIC es el de ecosistemas de innovación, concepto que viene de la política pública de ciencia y tecnología y que se relaciona con el concepto de “clusterización”, elemento que contribuye a que la innovación en seguridad digital se haga latente.

Posteriormente, el Dr. Bejarano dio la palabra al Dr. Mancipe, en lo atinente al artículo del Plan Nacional de Desarrollo que persiguió la creación de la Agencia Nacional de Seguridad Digital, principalmente se refirió a los pasos que seguiría la Presidencia de la República para la creación de tal Agencia, máxime cuando hay iniciativas legislativas que persiguen otras propuestas frente a la Agencia.

El Dr. Mancipe se refirió en primer lugar al trabajo legislativo que desde el gobierno se le ha dado a la creación de la Agencia. Sostuvo que desde Presidencia propusieron un nuevo articulado para la próxima legislatura de 2023, y lograr finalmente la creación de la Agencia a través de una ley de la república.

Hizo referencia al trabajo articulado que se ha desarrollado con embajadas de otros países en los que ya existe alguna entidad nacional que regule la seguridad digital y temas del espacio, quienes han dado la razón a Colombia en establecer como competente del manejo de la agencia a la Presidencia y no a un ministerio en concreto, pues es un tema de política pública de la mayor relevancia de cara al futuro.

De otro lado, habló sobre la constitución de la Agencia, en el sentido en que, en materia de seguridad, hay un área dedicada a la seguridad digital destinada a apoyar a todas las instancias, velaría por el cumplimiento de la normatividad relacionada con el tema (protección de datos, gobernanza, uso de la información, etc.). También hay un área dedicada al entrenamiento y a la capacitación. Se ha planteado la posibilidad de que COLCERT pase a ser parte de la Agencia y deje de pertenecer a MinTIC.

Cerrando el panel, el Dr. Bejarano destacó que Colombia ha planteado tres políticas públicas referidas a la seguridad digital, y preguntó si Colombia debería hacer una nueva política nacional o establecer una estrategia nacional.

Quien tomó la palabra primero fue el Dr. Palomá, considerando la segunda opción como la más viable para el país.

El Dr. Rodríguez también consideró mejor la implementación de una estrategia con la participación de todos los sectores relevantes.

El Dr. Salazar estuvo de acuerdo con sus compañeros de panel, añadiendo que la estrategia debería revisarse y analizarse periódicamente, sugiriendo un plazo de 2 años.

Finalmente, Julio César Mancipe sostuvo que la mejor alternativa sería la estrategia que persiga la mitigación de ciberataques, pues actualmente las políticas públicas existentes se han quedado cortas para tratar la ciberdelincuencia, por lo que la estrategia sería la mejor respuesta.

Conferencia: Sobre la creación de la Agencia de Ciberseguridad y Asuntos Espaciales

Conferencista:

Lina Areng – Líder del programa regional Centro de Competencias y Ciber capacidades de Latinoamérica y el Caribe (LAC 4), Unión Europea.

La Dra. Areng sostuvo que el propósito de LAC 4 es mejorar las capacidades regionales en ciberseguridad y ciberdelincuencia, lo que permitirá mejorar los medios a través de los cuales los gobiernos y organizaciones aseguran tecnologías que juegan papel fundamental en la vida cotidiana.

Sostuvo que todos los países han sido golpeados en temas de ciberseguridad, tanto en Latinoamérica como en Europa, lo que afecta la confianza en la sociedad digital. Colombia cuenta con un modelo de gobernanza con una variedad de actores y funciones, pues de un lado tiene órganos como MinTIC, la Unidad de Delitos Informáticos de la Fiscalía, COLCERT, entre otros. Además, cuenta con convenios nacionales e internacionales contra la ciberdelincuencia y en temas de seguridad digital. Sin embargo, la aplicación de estos instrumentos no ha sido tan expedita ante la falta de coordinación de las instancias creadas al interior del país, así como la falta de asignación presupuestal destinada al sector.

Señaló que, ante este panorama, la creación de la Agencia Nacional de Seguridad Digital es clave para que funja como la máxima autoridad para la formulación y aplicación de las estrategias nacionales y políticas en materia digital, lo que sería un factor diferenciador para mejorar la seguridad digital de Colombia.

Con base en la experiencia de LAC 4, un elemento clave para fortalecer la ciberseguridad en el país es contar con una autoridad que regule estos temas. Ello implica que actúe como entidad gestora para aclarar los procesos y las tareas necesarias para garantizar una postura eficaz en materia de ciberseguridad.

Se refirió a algunos países que cuentan con este tipo de autoridades, como Países Bajos, Estonia y República Checa. Dijo que estos organismos son la máxima instancia en materia de ciberseguridad en esos países, lo que ha fortalecido y potencializado el sector de la ciberseguridad a nivel nacional e internacional, permitiendo un mayor nivel de cooperación entre actores, creando mecanismos ágiles y eficientes ante las amenazas digitales que se presentan.

Por lo anterior, la Dra. Areng celebró la introducción del proyecto de ley en el Congreso de la República colombiano que persigue la creación de la Agencia Nacional de Seguridad Digital, lo que contribuirá a organizar y crear estrategias para fortalecer las políticas públicas sobre ciberseguridad en el país.

Ahora bien, sobre el proyecto de ley realizó una serie de observaciones que desde LAC 4 sugieren a Colombia. Por ejemplo, sobre el artículo de definiciones sugirió modificar los conceptos de ciberseguridad y ciberataque, debido a que estas definiciones se refieren a la seguridad nacional, y resaltó que en derecho internacional hay una diferencia importante entre ellos y el concepto de ataque se emplea ante situaciones más extremas de seguridad. Por esto, sugirió sustituir los conceptos por las palabras amenaza o incidente.

Además, sugirió agregar un apartado en el que se promuevan las reuniones intersectoriales, tanto a nivel privado como público para obtener resultados integrados, armónicos y concertados. Asimismo, destacó la creación del Fondo Nacional para la Seguridad Digital, pues desde LAC 4 han visto que varios países se afanan en la creación de organismos y estrategias nacionales, pero al momento de implementarlos no cuentan con los recursos suficientes, lo que hace que los esfuerzos por mejorar y fortalecer la seguridad digital queden rezagados.

Por último, concluyó su exposición mencionando que, en virtud del mandato de LAC 4 como uno de los principales representantes de la Unión Europea en ciberseguridad, estarían apoyando con todo el gusto en formación y capacitación para la consolidación de la Agencia Nacional de Seguridad Digital en el país.

Panel: Gobernanza de la seguridad digital y mecanismos de interacción entre agentes

Moderadora: Carmen Ligia Valderrama – Exministra TIC, experta en TIC y docente de la Universidad Externado de Colombia

Panelistas:

Carolina Botero – Directora de la fundación “Karisma”

Orlando Garcés – Oficial del programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la OEA

Santiago Pinzón – Vicepresidente de Transformación Digital de la ANDI

Iván Durán – Alto Consejero TIC de Bogotá

Inició la moderadora destacando el fomento de estos espacios de discusión sobre temas de tan alta relevancia para la cotidianidad actual, tanto nacional como internacional.

Sostuvo que el panel tiene como propósito tocar dos temas: el de la gobernanza y el de la participación de los agentes en la seguridad digital y la ciberseguridad.

Hizo un llamado a tener presente que la gobernanza se relaciona con la forma en que se concibe la política en un tema particular, y para el caso de este panel, se referirá a la forma de abordar la política de ciberseguridad.

En el caso de la gobernanza, se refirieron los panelistas a cómo se está implementando la política en los estados americanos, principalmente desde una visión de prevención más que de reacción. Además, sostuvo que además del CONPES, en Colombia el Decreto 338 de 2022 aportó un esquema de gobernanza digital claro.

En primer lugar, intervino el Dr. Garcés para mencionar la tendencia internacional frente a la gobernanza digital, cuáles han sido los avances y qué políticas han adoptado los estados americanos.

El panelista mencionó que desde la OEA y en concreto desde la CICTE, han venido apoyando a la región desde políticas y estrategias nacionales en clave de ciberseguridad. La OEA ha sido muy cercana a Colombia y ha estado atenta a sus políticas y medidas internas. Sostuvo que alrededor de 19 estados miembros que han expedido estrategias políticas nacionales alrededor de la ciberseguridad. Es así como en Colombia se han implementado políticas nacionales para fortalecer la seguridad digital. Colombia es el único país en la región que ha tratado el tema por medio de tres políticas nacionales, otros lo han hecho a través de estrategias o planes nacionales.

Sostuvo que el ecosistema de ciberseguridad tiene varios enfoques, pero desde la gobernanza es clave hablar de las personas y las organizaciones, pues hay países que van más avanzados que otros en modelos de gobernanza, como por ejemplo República Dominicana, que es el más adelantado en la región de Latinoamérica y el Caribe.

Resaltó dos asuntos clave que para la OEA son imprescindibles como lo son la cooperación internacional y la ciberdiplomacia. Un marco de gobernanza debe incorporar un análisis detallado no solamente de los asuntos nacionales, sino de los internacionales y globales en torno a la temática. Destacó que la región de América Latina ha tomado decisiones en muy corto plazo en donde los países han logrado acuerdos para fomentar y fortalecer la confianza, lo cual es celebrado por parte de la OEA. Esto buscó aportar a la estabilidad en el ciberespacio.

Terminó mencionando varias medidas que se han tomado, como por ejemplo, la inclusión de la mujer en el sector, se implementó un repositorio de información a cargo de la OEA donde constan todas las políticas y estrategias que han incluido los países en sus planes de gobierno, entre otras.

La Dra. Valderrama retomó el uso de la palabra para decir que la confianza es fundamental, pues la ciberseguridad va de la mano con la confianza, pues es justamente lo que se ha quebrantado con los ciberataques.

Continuó el Dr. Iván Durán, quien habló sobre la gobernanza vista desde el gobierno, especialmente lo referido al CONPES de 2016 y al Decreto 338 de 2022, es decir, lo atinente a las políticas de gobierno. El Dr. Durán mencionó que el apoyo de la OEA ha sido clave para que Colombia avance por buen camino en materia de ciberseguridad. Agregó que ha sido un trabajo de diseño de política pública que derivó en el Decreto 338 de 2022, el cual ha sido muy bien acogido en el sector.

Manifestó que esta ha sido una evolución de política pública con intervención de actores nacionales e internacionales, que conduce a que los objetivos que se plantean se vayan materializando. Consideró que el modelo de gobernanza del país es un modelo que formalizó muchas cosas que eran necesarias en el país, como la creación del COLCERT, de tener una metodología de identificación de infraestructuras críticas cibernéticas de la mano del sector civil, no solo del sector defensa, entre otras.

Ahora bien, habló sobre Bogotá, en tanto ha sido muy juiciosa en seguir los lineamientos de la política digital que derivó en el Decreto 338. Asimismo, sostuvo que está desarrollando protocolos de gestión de incidentes muy alineados con lo producido por MinTIC con base en algunas normas.

Agregó finalmente que la gobernanza del país en materia de ciberseguridad ha tenido gran apoyo internacional, pero que tiene el reto de volverse aun más operativa y dinámica.

La moderadora destacó que la gobernanza es un proceso, siguiendo con las palabras del Dr. Durán, pues no se pueden generar situaciones de la noche a la mañana, sino que es un proceso en el que Colombia va por buen camino, pues ha tenido una regulación importante y acertada frente al tema, lo que no significa que no se existan retos por delante.

Además, manifestó que no solamente el gobierno hace parte de toda la gobernanza en materia de seguridad digital, sino que los empresarios también son protagonistas. El Foro Económico Mundial indicó que para el 2021 el 74% de las empresas estaban en alto riesgo de ser hackeadas, lo que no significa que el 26% restante estuviese seguro, sino medianamente con menor riesgo. Esta cifra es bien preocupante y alarmante, y la Dra. Valderrama indicó que es una situación que ocurre en varios sectores como en el de salud.

Lo anterior fue para introducir al siguiente panelista, el Dr. Santiago Pinzón, representante de la ANDI, quien habló sobre la ciberseguridad en la red empresarial actual.

El Dr. Pinzón inició su exposición trayendo a colación el Decreto 2647, que fue el que reestructuró el Departamento Administrativo de la Presidencia (DAPRE), y hay un artículo específico en el que el director del DAPRE tiene la función de asesorar al Presidente en la implementación de estrategias en materia de seguridad digital y ciberseguridad.

De otro lado, habló sobre la creación de la Agencia Nacional de Seguridad Digital, lo que terminaría permeando también al sector privado, pues habría que ver dónde está la gobernanza, si en Presidencia o si en una entidad aparte.

Además, señaló que la ANDI ha ido recogiendo información con los distintos empresarios relacionada con ciberseguridad. Por ejemplo, dio una cifra de denuncias que recibió la Policía Nacional en 2021 sobre ciberataques, la cual fue de 54.000, de donde la mayor parte fue por suplantación, y es lo que más se ve en el sector empresarial, tanto en grandes como en medianas y pequeñas empresas.

Indicó que las Pymes no le prestan atención a la ciberseguridad, por desconocimiento y por falta de recursos, pues no es algo que vean como relevante a la hora de estructurar y poner en operación sus empresas. La ciberseguridad es más de empresas grandes y entidades ya consolidadas en un mercado.

Destacó que es un tema de interés general, no solo algo del gobierno, sino un tema para toda la sociedad y comunidad civil, pues hoy por hoy es algo del que nadie es ajeno. Por esto, celebró estos espacios de discusión y debate desde una visión pública pero también privada y desde la empresa, pues el trabajo articulado entre ambos sectores ha conllevado a la implementación de medidas y políticas positivas para el país en estos aspectos cibernéticos.

La Dra. Valderrama dio la palabra a la Dra. Botero para que hablara de la ciberseguridad en la vida del ciudadano de a pie colombiano, especialmente enfocado a los derechos humanos.

La representante de la fundación Karisma comenzó diciendo que Colombia ha sido un líder en la región en materia de seguridad digital, lo que denotó el peso que este tema tiene en el ámbito militar. Precisamente fue este el fundamento del CONPES 2011, pues hubo una disputa en el terreno democrático que involucró la seguridad nacional.

Indicó que la ciberseguridad se ha planteado en términos militares principalmente, con una participación fundamental e integral de las empresas, pero con un desconocimiento abismal por parte de las personas, de la sociedad civil, y en últimas son ellas las destinatarias de las políticas públicas. Dio el ejemplo de cuando las mujeres son víctimas de ciberataques cuando se difunden fotos íntimas de ellas sin su consentimiento, y ese es un caso no solo de derechos fundamentales menoscabados, sino un tema de seguridad digital del cual la sociedad civil no tiene conocimiento suficiente para contrarrestar. Para solucionar esto, propuso recolectar cifras con enfoque diferencial,

centrándose en poblaciones históricamente discriminadas (mujeres, comunidades indígenas y afrodescendientes, población LGBTIQ+), no solo quedarse en temas militares y empresariales, sino ampliar el espectro de protección.

El Dr. Iván Durán replicó a la anterior conferencista, manifestando su acuerdo con su visión. Indicó que un psicólogo lleva un buen tiempo diciendo que las mujeres adolescentes son las más vulnerables digitalmente, por diversos factores.

Igualmente, el Dr. Pinzón también manifestó su acuerdo con la Dra. Botero, resaltando que actualmente hay muchos sectores y grupos que deben tenerse en cuenta para realizar métricas y estadísticas en clave de ciberseguridad. Además, se refirió a la Comisión accidental en Ciberseguridad que se creó en la Cámara de Representantes y próximamente se creará en el Senado, pues las unidades de trabajo legislativo no tienen tampoco el pleno conocimiento en ciberseguridad, por lo que la especialidad y la capacitación en estos temas, incluso en el Congreso, es fundamental.

Replicó la Dra. Botero y habló sobre el sexting, en el sentido en que esto no es un delito, pues el sexting es algo que la gente puede hacer, y en ocasiones se convierte en un delito, pero la visión de MinTIC frente a esto no ha sido la más apropiada, señaló la expositora.

La Dra. Valderrama abordó una temática que trató la anterior panelista, en el sentido en que existe dificultad en considerar qué es un ciberdelito, pues no se sabe desde donde y hasta qué punto hay un ciberdelito, pues la línea es bastante delgada, y este ha sido un reto para el gobierno, en particular para MinTIC.

El Dr. Garcés inició la segunda ronda de preguntas relacionada con la intervención de los distintos agentes. Señaló que ha habido tres etapas de políticas o estrategias nacionales de ciberseguridad: en la primera (2010-2015) se reactivó el liderazgo del sector militar; en la segunda, es decir de 2015 a 2020 se ha hecho un enfoque en gestión de riesgos en seguridad digital, se tocan temas de ciberdiplomacia y fortalecimiento de capacidades; y la tercera, que inició en 2020 hasta la actualidad, en donde se rescatan y resaltan temas frente a la gobernanza, pero desde distintos enfoques.

Rescató que uno de los grandes proyectos que está desarrollando la OEA en ciberseguridad persigue la promoción la perspectiva de género en la agenda de ciberseguridad de la región. Han trabajado en las políticas de ciberseguridad rescatando componentes de diversidad e inclusión social y poniéndolos como prioridad.

El Dr. Durán concluyó su intervención dando algunas cifras en Bogotá, en donde alrededor del 30% de los ciberataques ocurren en esa ciudad, por su gran amplitud territorial. Sostuvo que hay varias entidades atacadas constantemente, especialmente aquellas que manejan información sensible. Sin embargo, Bogotá ha sabido contrarrestar tales amenazas, particularmente porque ha sido muy unida a MinTIC en la mitigación de

dichos ataques. Concluyó diciendo que Colombia gracias a la OEA, al sector privado y a la sociedad civil, ha tenido aportes muy grandes y unos marcos de política y estrategias muy interesante y vanguardista. Lo que se pretende, señaló Durán, es operativizar todos estos temas y materializarlos en la práctica.

Tomó la palabra el representante de la ANDI, quien indicó que hay un reto enorme en materia de ciberseguridad, especialmente porque hay un 40% de empresas que no tienen un esquema de seguridad digital, lo cual debería ser una cifra mucho menor. Además, insistió en el tema del mantenimiento de la capacidad institucional, pues en Colombia falta llevar a ejecución varios planes, lo cual podría reducirse, o más bien, mejorarse, brindándole un enfoque de Estado y fortaleciendo la institucionalidad. Y finalmente, dijo que hay un gran desafío en el tema de talento, para lo cual dijo que el rol del SENA es esencial, quien debe echarse al hombro la función de capacitación y de enseñanza en estos temas cibernéticos, cuya oferta actual no está muy elevada en esa entidad.

Cerró el panel la Dra. Botero, resaltando la importancia de abrir espacios para la sociedad civil, la cual debería ser muy tenida en cuenta por parte de los reguladores, pues se adquieren nuevas perspectivas y nuevos puntos de vista que contribuyen a un fortalecimiento de las estrategias de seguridad digital de la nación. Además, habló de la importancia de incorporar la perspectiva de derechos humanos a la hora de capacitar a personas en seguridad digital y ciberseguridad, pues no todo son aspectos técnicos o económicos, sino que también hay que tener en cuenta un componente humano.

La Dra. Valderrama agradeció a los panelistas y resaltó la cantidad de retos y desafíos que se vienen por delante en materia de políticas, estrategias y proyectos en ciberseguridad, y cuyo éxito se obtendrá, en gran parte, si se trabaja de la mano con la gobernanza digital integral.

Conferencia: Habilitadores y dinamizadores de las capacidades en seguridad digital para el país

Conferencista: Juan Pablo Salazar – Experto en materia TIC y docente

Inició mencionando que actualmente nos encontramos en una evolución de lo digital, pues ya estamos en la etapa de las tecnologías emergentes (5G). Sostuvo que hay un real cambio de todas las competencias de las personas, donde la automatización está incidiendo mucho más en los modelos de negocio, la realidad virtual, la inteligencia artificial y la realidad aumentada están impactando mucho y creciendo cada vez más.

Todo lo anterior es solo una introducción para evidenciar que la vida en el mundo digital ha migrado y ha mutado, mostrando cómo la tecnología transforma la productividad y la forma de ver el mundo.

A pesar de todo este avance tecnológico, digital y robótico, el conferencista mencionó que no estamos preparados para afrontar los retos presentes y futuros de la ciberseguridad en Colombia, como por ejemplo para la economía digital.

En primer lugar, porque existe una desalineación de objetivos en cuanto a políticas normativas, herramientas público-privadas y frente a la institucionalidad, muy a pesar de que el país ha sido líder en la ciberseguridad en la región.

Entró a hablar de los dinamizadores de la ciberseguridad en Colombia, y sostuvo que para tener una política pública de Estado sólida en ciberseguridad y ciberdefensa se requiere de cuatro elementos fundamentales: tener un contexto, una regulación, unas instituciones y unas herramientas adecuadas, lo cual debe lograr una coordinación público-privada efectiva, una alineación de esfuerzos público-privados, la defensa de los derechos de las personas y una alineación en infraestructuras críticas.

Frente al contexto, el Dr. Salazar sostuvo que cada decisión que se tome en materia de ciberseguridad debe tener en cuenta la tecnología existente y la futura. Además, analizar cuáles son los negocios y el uso que se les da y la apropiación que de lo anterior tiene el país. Sostuvo que el internet claramente ha evolucionado, como que por ejemplo en EE. UU un robot periodista fue acusado de racismo, lo cual era algo impensable hace unos años. Del mismo modo, ha cambiado la forma de pago, como se ha ido abriendo camino la realidad aumentada y muchas cosas más que han modificado la forma de vivir hoy por hoy.

Señaló que la web también ha evolucionado, pues antes era una web absolutamente centralizada donde el usuario era un simple consumidor. Luego pasó a ser también productor, sin dejar de ser consumidor, en una web centralizada a la cual se le añadieron las redes sociales. Y, por último, llegó una web absolutamente descentralizada donde el usuario es consumidor, productor y además dueño del mundo digital en tanto invierte en él a través de los criptoactivos, del blockchain, etc.

De otro lado, mencionó que la política internacional ha evolucionado, y muestra de ello es que la independencia, bajo la óptica del derecho internacional, implica el derecho a ejercer en ella las funciones de un Estado, con exclusión de cualquier otro Estado, y esto, en el mundo digital, involucra personas y un territorio particular, que es el territorio de lo cibernético, es decir un territorio no físico sino digital.

La soberanía de los Estados implica la existencia de un ciberespacio que vincula a personas, infraestructuras, dispositivos y datos, los cuales tienen como base el funcionamiento de la internet.

Todo lo anterior para ejemplificar que la soberanía en lo digital es muy compleja y problemática. Dio como ejemplo que un delito se cometió en el país 1, los servidores y el host están en el país 2 y los ciberdelincuentes en el país 3, lo cual ocurrió en el Puerto

de Amberes, Bélgica. Estos son los retos que afrontan los estados con la ciberseguridad, los cuales son muy complejos de solucionar y contrarrestar.

Continuó con su exposición para ahora tratar los principios y elementos de la cibersoberanía. Sostuvo que el Estado ejercer soberanía sobre las personas involucradas en ciber actividades en su propio territorio, así como ejerce tal soberanía sobre ciber actividades originadas en su territorio o completadas en él, lo que persigue un efecto de territorialidad y extraterritorialidad de la soberanía. Todo lo anterior está en el Convenio de Budapest, el cual fue aprobado y ratificado en Colombia a través de una ley.

Se refirió a la proliferación de ciberataques desde los años 90, donde ha habido más de 50 alrededor de todo el mundo.

Luego, se refirió a la regulación en lo relacionado con el modelo de seguridad y privacidad de la información, gobierno de datos, regulación por cada sector y las diversas convenciones internacionales. Señaló que en Colombia no hay un objetivo coordinado en punto de ciberseguridad, por eso consideró que hay una regulación desalineada. Sostuvo que MinTIC ha buscado mantener la confianza de la gente y las políticas públicas han servido mucho, pero en el sector privado no se corre la misma suerte.

Destacó, por dar algunos ejemplos, varias resoluciones y otros instrumentos que han sido expedidos en Colombia para regular los temas anteriormente dichos. Así, desde 2011 ha habido 3 CONPES, resoluciones sobre seguridad web y sobre sedes eléctricas, una resolución sobre el Plan Nacional de Infraestructura de Datos, resoluciones de la CRC, instrucciones de las Superintendencias (Financiera y de Industria y Comercio), 24 guías y 2 modelos en materia de modelo de seguridad y gobierno digital y una convención que forma parte del bloque de constitucionalidad colombiano.

Ahora bien, frente a las instituciones, el Dr. Salazar mencionó que ha sido un trabajo conjunto de la Presidencia de la República, de MinTIC, de la ANE, de COLCERT, del Ministerio de Defensa, de la SIC, de la Fiscalía, entre otros.

Finalmente, en la última dimensión de habilitadores y dinamizadores de la ciberseguridad, están las herramientas. Hay que partir de que la motivación que llega a realizar un ciberataque es distinta en cada caso y hay que tener un modelo o una forma de protección diferente para cada ataque cibernético. El conferencista sugirió tener un enfoque multidimensional de la ciberseguridad para mitigar cualquier clase de ataque, para lo cual hay diversas herramientas como consejos nacionales de seguridad digital, tipificar un régimen sancionatorio, hacer evaluaciones o assessments previos, adherirse a los protocolos de Budapest, establecer un régimen de interconexión para la ciberseguridad, competencias en infraestructura crítica, entre otras.

Conferencia: Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talentos y habilidades

Conferencista: Orlando Garcés – Oficial del programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) de la OEA

Indicó que hablaría sobre un reporte que realizó la OEA sobre el desarrollo de la fuerza laboral en materia de ciberseguridad. Mencionó que en el programa de ciberseguridad del CICTE de la OEA tienen tres enfoques: i. Desarrollo de capacidades, en donde apoyan a los varios países de la región en la implementación de políticas y estrategias nacionales en ciberseguridad; ii. Fortalecimiento de capacidades. Esto es clave, porque aquí hay capacidades técnicas y varios equipos de respuesta ante incidentes nacionales sobre ciberseguridad, a los que Colombia se conectó hace poco; iii. Investigación y propagación del conocimiento.

Luego, el Dr. Garcés se refirió al reporte propiamente. Destacó que se dividió en cuatro partes, en donde la primera se trataba sobre el contexto actual de la ciberseguridad para identificar las condiciones actuales en el mercado laboral de ciberseguridad. De ahí pasó a la segunda parte, pues todo ese contexto definió lo que es el mercado laboral de ciberseguridad y la fuerza laboral de ciberseguridad. Tercero, el análisis lo hicieron desde el lado de la demanda como del lado de la oferta, así como identificaron una serie de retos y desafíos que tiene la región, para así pasar a la cuarta parte del reporte, es decir, un llamado a la acción.

Resaltó que los países de la región ya son bastante maduros en punto de ciberseguridad, en el sentido en que tienen formulación de políticas y estrategias nacionales, pero falta volverlas operativas en un 100%.

Posteriormente, indicó que la pandemia del COVID-19 cambió totalmente la forma en que se trabaja, pues el teletrabajo y los modelos híbridos explotaron y son lo más común hoy por hoy. Sin embargo, esto dejó también un alto desempleo, una brecha de género mucho más grande de la que existía. Además, la alta digitalización generó una serie de efectos, pues desde las pequeñas, medianas y grandes empresas ha habido reacciones frente a esta era digital, lo que ha generado una presión grande en las organizaciones y en los países para obtener profesionales en seguridad.

Para abordar el tema, el Dr. Garcés dijo que tocaba definir la fuerza laboral, eso es lo primero y lo fundamental. Por ejemplo, en EE. UU han encontrado 52 tipos de fuerza laboral o de roles laborales en el marco de la ciberseguridad, lo que ha sido un trabajo conjunto del sector público con el privado.

Además, sostuvo que el mercado de la ciberseguridad se rige por dos fuerzas como todo mercado: oferta y demanda. La oferta en el mercado laboral de ciberseguridad la conforman estudiantes, aprendices, profesionales de otros sectores que quieren

capacitarse en ciberseguridad y solicitantes de empleo. En la oferta están las escuelas, los institutos, las universidades, es decir, la academia en general. Por el lado de la demanda, están las organizaciones en general, tanto públicas como privadas y de otra índole. Dentro de estas organizaciones están las áreas de recursos humanos y las juntas directivas que son los órganos fundamentales.

Hay muchos retos desde la oferta, desde la demanda y desde los gobiernos. Desde la oferta la OEA identificó varios retos en la región de América Latina y el Caribe: hay insuficiente desarrollo en las carreras STEM en materia de ciberseguridad y una baja vocación para infundir habilidades en temas digitales desde las escuelas; hay un bajo y mediano nivel de inglés en la región, lo que impide muchas veces el acceso a la ciberseguridad, pues el lenguaje predominante allí es el inglés; falta de sensibilización y de educación en edad temprana en temas digitales y de ciberseguridad; hay un desconocimiento de las oportunidades educativas que tienen los estudiantes y no hay una comprensión sobre la definición de la profesión de la ciberseguridad, entre otras.

Desde el punto de vista de la demanda, los retos se refieren a que no hay un lenguaje común en el mercado; las organizaciones prefieren experiencia sobre las certificaciones de los postulantes; hay unas brechas gigantes en temas de diversidad, inclusión social e identidad de género; hay dificultades en acceder a los marcos de trayectoria profesional, pues hay cursos y certificaciones muy costosas, lo que le queda difícil a la mayoría de postulantes, que son estudiantes recién graduados y que apenas están teniendo sus primeros acercamientos con el mundo laboral.

Finalmente, el Dr. Garcés indicó que el reporte terminó con una serie de recomendaciones para los gobiernos y los distintos actores, entre las cuales se tiene que debe haber un marco claro de gobernanza, y al tenerlo claro, debe pensarse en estrategias nacionales para el desarrollo de la fuerza laboral en ciberseguridad y hacer proyecciones tanto desde la demanda como desde la oferta. Insistió en la necesidad de establecer relaciones o alianzas público-privadas que contribuyan a adaptar y robustecer los marcos regulatorios y legislativos.

El evento finalizó con la presentadora dando las gracias a todos los asistentes, panelistas y demás interesados por haber participado en el evento.