# ‘Estado de la Ciberseguridad en Colombia’


**Departamento de Derecho, Comunicaciones y Tecnologías de la Información.**

**Universidad Externado de Colombia**

**23 de abril de 2025**

**Bogotá D.C., Colombia**

**Compilado por**:

Ana María Alba Medina

**Universidad Externado de Colombia**


Calle 12 No. 1-17 Este
Bogotá, D.C., Colombia

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

**Apertura e Instalación del Evento**

**Intervención Dra. Sandra Ortiz Laverde – Directora del Departamento de Derecho, Comunicaciones y Tecnologías de la Información**

La Dra. Sandra inició con el agradecimiento a los asistentes presenciales y virtuales. Prosiguió con una breve presentación del evento, para lo cual explicó que el estudio objeto del evento, fue elaborado por la Cámara Colombiana de Informática y Telecomunicaciones y su centro de pensamiento tictac. Dicho estudio sobre el estado de la ciberseguridad de la IA en Colombia. El cual consta de 5 partes que fijan el panorama general del ecosistema digital en Colombia, en lo relativo a las políticas públicas que se han desarrollado.

**La Agenda Académica del Evento:**

| HORA | TEMA |
|---|---|
| **7:30 a.m a 8:00 a.m** | Registro de asistentes |
| **8:00 a.m. a 8:15 a.m.** | **Instalación y consideraciones de apertura:**<br><br>**Sandra Ortiz Laverde.** Directora Departamento de Derecho, Comunicaciones y Tecnologías de la Información – Universidad Externado de Colombia. |
| **8:15 a.m. a 9:00 a.m.** | **Presentación Estudio – Estado de la ciberseguridad en Colombia** |

| | |
|---|---|
| | **Germán López Ardila.** Vicepresidente Legal – CCIT. |
| **9:00 a.m. a 10:00 a.m.** | **Conversatorio**<br>**Panelistas:**<br>• Pedro Romero. Oficial de Privacidad y Cumplimiento de Huawei.<br>• Emanuel Ortiz. Director del Programa de Gerencia de Ciberseguridad Universidad EAN.<br>• Coronel Nelson Tapia. Comandante del Comando Conjunto Cibernético de las Fuerza Militares de Colombia.<br><br>**Moderadora:** Sandra Ortiz Laverde. Directora Departamento de Derecho, Comunicaciones y Tecnologías de la Información – Universidad Externado de Colombia. |
| **10:00 a.m. 10:10 a.m.** | **Conclusiones.** |

**Intervención Dr. Germán López – Vicepresidente Cámara Colombiana de Informática y Telecomunicaciones.**

Para comenzar, el Dr. Germán señaló que en el panorama general del país en temas de ciberseguridad y de inteligencia artificial. Señaló que lo que se busca con el estudio es construir un insumo que recopile los elementos base del ecosistema digital y de ciberseguridad en Colombia. Adicionalmente, que se evidencia el aumento de los de las ciber denuncias y los ciberataques que está sufriendo Colombia, uno de los países más afectados en América Latina, especialmente después de la pandemia, como consecuencia de la aceleración de la digitalización, que hizo que las interacciones se trasladaran al entorno digital cada vez más, lo que se traduce a que los delincuentes empleen estos medios para realizar actividades ilegales.

Sobre el análisis del índice de ciberseguridad, señaló que la UIT lo lleva a cabo a través de 5 dimensiones o pilares claves: (i) marco legal del país acerca de la protección de datos, (ii) existencia de medidas técnicas para atender incidentes según las capacidades técnicas del país; (iii) capacidad de los actores de interactuar y articularse entre sí, (iv) desarrollo de capacidad de talento humano y (v) existencia de medidas de cooperación internacional.

Lo anterior, arroja para Colombia múltiples desafíos. En primer lugar, la baja implementación de políticas de ciberseguridad, cuyo desarrollo debe hacerse no solo por el gobierno, sino también por el sector privado, y en segundo lugar, la existencia de una brecha entre el gobierno nacional y los gobiernos municipales y departamentales, que tienen que articularse para que sea posible unificar los esfuerzos, y así, dar cumplimiento a la política de gobierno digital.

Ahora bien, en cuanto a las políticas de seguridad, estableció que si bien en el país existen leyes como la 1581 de 2012 o 1273 de 2009, es importante destacar también es esfuerzo que desde el 2011 se realiza con los documentos CONPES, que han permitido ver la importancia de que en la conversación acerca de la ciberseguridad se vean incluidos más actores.

Adicionalmente, comentó que Colombia cuenta con la Estrategia Nacional de Seguridad Digital, construida con la Organización de Estados Americanos (OEA) y que traza la hoja de ruta acerca de lo que debe pasar con la ciberseguridad a corto y mediano plazo. Este plan, también busca fortalecer la seguridad digital del país a través de unos lineamientos que permitan proteger infraestructuras críticas e impulsar el talento humano, promover la innovación y garantizar la protección y la confianza del ecosistema digital.

Con todo, concluyó que el diagnóstico de ciberseguridad en Colombia es positivo, resultado que se refleja gracias a los esfuerzos realizados por los diferentes actores intervinientes en los últimos años. Sin embargo, sigue siendo necesario materializar lo que está en el Plan Nacional de Desarrollo 2022-2026, particularmente en lo relacionado con los espacios de transformación digital

pública y de adopción de capacidades de ciberseguridad en la administración pública.

**PANEL ESTADO DE CIBERSEGURIDAD EN COLOMBIA**

1. **¿Cómo puede abordarse el tema del talento humano en el sector, teniendo en cuenta que es uno de los factores más importantes de la seguridad digital?**

Inició la Dra. Ingrid Hernández, asesora de transformación digital de la Presidencia de la República, respondiendo la pregunta. Al respecto, mencionó que el talento es uno de los desafíos más importantes en materia de ciberseguridad en Colombia, no solo en lo relativo al componente especializado y técnico, sino también a la concientización y cultura digital, frentes en los cuales hay que trabajar. Para esto, compartió que si bien la Estrategia de Seguridad Digital contemplada plantea como solución la creación de programas nacionales e integrales de educación y formación en seguridad digital, en los diferentes niveles, aún falta establecer cómo se implementará esta idea.

En segundo lugar, intervino el Dr.  Pedro Romero, oficial de protección de datos y ciberseguridad de Huawei Colombia. Quien respondió que actualmente existen muchos esfuerzos para mermar dicha problemática, para ejemplificar, compartió que existe en el Ministerio de Tecnologías de la Información y Comunicaciones (MinTic) un programa llamado ‘Avanza TEC’, donde las personas pueden capacitarse de la mano de las empresas, porque gran parte de las empresas de tecnologías necesitan talento que sepa y domine el tema. Para destacar la importancia de estas iniciativas, advirtió que una empresa de tecnología que no cuente con talento humano de calidad no es nada. Desde Huawei se tiene un programa denominado ‘ICT Academy’, una academia de las TIC que en alianza con universidades, crea nuevos talentos. Resaltó que la importancia de estas iniciativas radica en la poca disponibilidad de personas especializadas en la materia, a pesar de la alta demanda de conocimiento de ese tipo.

En tercer lugar, el Dr. Emmanuel Ortiz, director de la especialización de ciberseguridad de la Universidad EAN añadió a la discusión que es necesario guardar pertinencia frente a nuestro contexto global de ciberataques. Aterrizado al escenario nacional, ya que existe una falencia en la creación del talento humano, en tanto se cultivan los conocimientos basados en las habilidades generales requeridas, pero no las específicas. Por ello, no se ve optimizado el talento existente, lo cual va en detrimento de su permanencia económica y social a futuro. Adicionalmente, hace una crítica acerca del verdadero valor que tienen las certificaciones, que bajo su perspectiva, no bastan en materia de habilidades de poder, que son las que permiten a la persona realmente optimizar su valor.

Finalmente, participó la Dra. Sandra Ortiz Laverde, quien concluyó que como país, lo que debemos hacer es identificar hacia dónde debe estar orientado nuestro talento en función de las discusiones propias del ámbito local, y así, las necesidades que surgen de ellas. También mencionó que el Estado eventualmente puede requerir del sector privado, como se evidenció en el ciber ataque de hace 2 años, por lo que es necesario que las entidades públicas capaciten a sus funcionarios, para que estos también puedan dar respuesta a lo que está pasando.

2. **Se ha dicho que la ciberseguridad, eminentemente, es un diálogo entre distintas partes interesadas. Esto nos lleva a mantener, por un lado, la conversación nacional acerca de institucionalidad y gobernanza, y por otro, la conversación internacional acerca de la cooperación con los demás Estados, que también enfrentan amenazas de carácter global. Con esto, ¿cómo creen que se puede fortalecer ese marco de gobernanza y conversación a nivel nacional? ¿cómo contribuye ese fortalecimiento interno a la cooperación y la actuación eficiente a nivel internacional?**

La pregunta fue respondida en primer lugar por el Dr. Emmanuel Ortiz, quien compartió que la tras nacionalidad de estos ciberataques, sumada a los contextos geopolíticos que vienen sucediendo a nivel global, llevan a reflexionar sobre lo que se está haciendo en Colombia y cómo se podría abordar el eventual

escenario de compartir información en tiempo real. Así, los focos o elementos de atención que permiten saber cómo actuar en caso de infraestructura crítica cibernética nacional, escenario en el cual lo más importante es la optimización del recurso de intercambio de información simultánea para anticiparnos a eventuales ciberataques, ya que existe una brecha en la anticipación por parte de herramientas de monitoreo y detección que actualmente se tienen a nivel global, lo cual representa un problema mayor si se tiene en cuenta que la cantidad de ataques digitales, y la sofisticación de los mismos, va constantemente en aumento.

Agregó que la cooperación internacional es supremamente necesaria como un factor de oportunidad, de necesidad y de cambio, aspectos en los cuales aportan la industria, la academia, y por supuesto, el Estado.

Finalmente, comentó que Colombia puede hacer muchas cosas para contribuir, pero que especialmente, debe centrarse en los puntos o ejes de enfoque necesarios y prioritarios en el presente.

A continuación, la Dra. Sandra por su parte señaló que, se puede abordar la respuesta desde dos ámbitos frente a este asunto. En el estudio es claro que se ha generado un marco normativo, pero aún falta la articulación de una entidad, como la que tiene Chile. Para ello, es importante analizar qué está sucediendo en la región a nivel de ciberseguridad, ya que siempre se tiende a mirar hacia la Unión Europea.  a nivel nacional es importante insistir en la creación de una agencia especializada en asuntos de ciberseguridad, con su respectiva delimitación de competencias y obligaciones que se deben reportar, observando cómo se articulan las demás entidades que han estado, porque existen una serie de CONPES que reflejan la continuidad de la política pública y los ejes que se han mantenido en lo referente a la confianza general que debe generarse en el ecosistema. Por otro lado, en el ámbito global, identificar las buenas prácticas y participar de las discusiones globales para traer al país los elementos que puedan servir.

Posterior a ello, la Dra. Ingrid Hernández mencionó que la cooperación internacional y la ciberseguridad están íntimamente relacionados con la forma en la que cada país emplea dicha herramienta con la finalidad de prepararse para un ciberataque. Es importante la comunicación de incidentes regionales para mitigar los ataques con mayor facilidad.

Para ejemplificar, compartió el ataque que sufrió en Colombia el proveedor de redes y servicios IFX. Relató que este ataque surgió inicialmente en Chile, que informó a través de Presidencia que la Agencia de Contratación Pública Chilena sufrió un ciberataque a través de su proveedor IFX, que, en cuestión de horas, se expandió a Colombia, generando la caída de los servicios de varias entidades de los sectores salud y judicial, lo que representó un daño menor gracias a la mitigación ejercida gracias a la comunicación anticipada.

Añadió que esta cooperación es fundamental para prevenir afrentas a la ciberseguridad y que hoy en día, Colombia no cuenta con ningún sistema que permita gestionar los riesgos, por lo que la creación de una entidad que se especialice en ese aspecto es imperativa. Se requiere una entidad que estructure, ejecute y complemente un esquema de gestión de los riesgos cibernéticos, pero también de la compartición de la información.

Señaló que la falencia que observa en la cooperación digital es la dispersión y fuga de esfuerzos, que de canalizarse, lograría una mayor efectividad y eficiencia, teniendo en cuenta que este no es una necesidad política, sino nacional y regional.

Cerró su intervención haciendo un llamado a la reflexión acerca de la figura del embajador de ciberseguridad, con el que ya cuentan múltiples países, y que los representa en los temas relativos a la seguridad, formando alianzas internacionales y manejando la ciber diplomacia del país de que se trate. También exhortó a la a la creación de la mesa táctica de academia y de gremios en el Comité Nacional de Seguridad Digital, para hacer una hoja de ruta de aquí al 2027 en el marco de la estrategia nacional digital.

Para concluir, el Dr. Pedro Romero se refirió al estado nacional de este diálogo, para lo cual comentó que si bien existen lineamientos nacionales claros en los CONPES y Planes de Desarrollo Nacional, sigue faltando la articulación y el esfuerzo unificado de todos los actores y las regiones para que se puedan lograr los objetivos nacionales a nivel de seguridad, ya que existen regiones que a hoy, adoptan menos de un 40% de los lineamientos o políticas de seguridad, mientras que otros el 70%.

Por otro lado, sobre los esfuerzos internacionales, agregó que Colombia está suscrita al Convenio de Budapest, y que si bien son útiles los esfuerzos coordinados desarrollados por diferentes entes internacionales, pero se requiere hacer un análisis de las mejores prácticas, tomarlas y ajustarlas a nuestra realidad y necesidades. Si los países latinoamericanos se unieran para trabajar los asuntos de ciberseguridad y protección de datos, se lograrían mejores resultados.

Para finalizar el panel, el Dr. Germán López reiteró la urgencia de crear una Agencia de Seguridad Digital, afirmando que este es un asunto de países, que debe ser atendido dada la exigencia del ecosistema al respecto.

Antes de concluir la sesión, se dio paso a algunas preguntas por el público. De las realizadas, se tomó la siguiente:

1. **Respecto del decreto 338 y desde la academia, ¿qué ha pasado con la infraestructura crítica y el impacto significativo de los umbrales, que tendría que establecer el Ministerio TIC para entender qué es un pacto significativo en un ciberataque en Colombia?**

La Dra. Ingrid Hernández respondió que desde la academia existen múltiples desafíos y frustraciones. El decreto 338 de 2022 establece toda la gobernanza en ciberseguridad y deja algunas tareas claras a algunas entidades, entre ellas MinTIC, que tiene una gran deuda relativa a la expedición en marzo de 2023 de una metodología para el mapeo de las infraestructuras críticas de Colombia, que nunca salió.

Destacó que en ciberseguridad, hablar de mora es crítico para la seguridad digital del país.

A continuación, el Dr. Pedro Romero resaltó que determinar la definición de infraestructura crítica es muy complicado, y que hoy en día debe incluso definirse como un servicio esencial. Hay que hacer un trabajo detallado, que incluye ver las aristas de cada una de las industrias para determinar si es o no una infraestructura crítica.

La Dra. Sandra extendió a los presentes la invitación a leer la tesis de un alumno de maestría, que explica por qué estamos en mora frente a las infraestructuras críticas. Adicionalmente, puntualizó que un gran problema que tenemos es que no hay continuidad en las políticas y los equipos y también que el Ministerio TIC tiene una sobrecarga de funciones, por lo que hay que preguntarse si la entidad está preparada para asumir más obligaciones y si tiene la suficiente planta para responder a lo que se le está asignando, teniendo en cuenta que puede ser el ministerio más transversal de todos.

El Dr. Emmanuel Ortiz reiteró que definir las infraestructuras críticas es un trabajo arduo éticamente y que la heterogeneidad de muchas de las estructuras, y sobre todo la disparidad en algunos estándares, implican un trabajo técnico muy agudo, por lo que unificar los temas de seguridad, de plataformas y de sistemas interconectados, es muy complejo.

Por último, retomó la palabra la Dra. Sandra para agregar que es la primera vez que se está abordando en redes sociales el tema de dónde navegan los niños y adolescentes. Frente a este, la CRC entiende que no se trata solo de los contenidos audiovisuales, sino también que los chicos manejan plataformas, por lo que es importante generar ambientes de discusión. Señaló que, si bien hace falta una competencia concreta en cabeza del regulador, hay un interés de generar los canales de denuncia que permitan exponer los delitos que se cometen con los menores.

**Cierre del evento**

Finalmente, el Dr. Germán López extendió su agradecimiento tanto a los expertos invitados, como al público presencial y virtual por su asistencia.