Colombia se prepara para **afrontar nuevos peligros**

El Gobierno está decidido a fortalecer la ciberseguridad y la ciberdefensa. María Isabel Mejía, viceministra TSI, habló sobre los proyectos que adelantan para ello. Representantes de sectores como el bancario, la industria y el Gobierno también contaron cómo avanzan en la tarea.

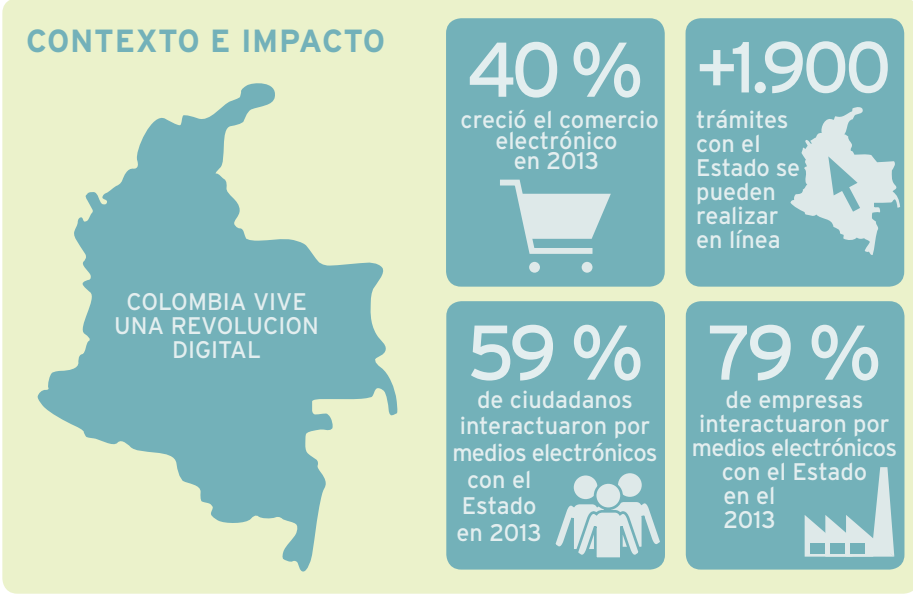
Colombia debe prepararse para afrontar los nuevos peligros del ciberespacio. Para ello, adelanta proyectos como la creación de una agencia coordinadora de las entidades de la seguridad y la defensa del país. Las acciones también incluyen el inventario y evaluación de las infraestructuras críticas, el fortalecimiento de la cooperación internacional y la actualización de la legislación en la materia.

Estos planes son el resultado de una política y una estrategia del Gobierno central. El Presidente de la República pidió a los ministerios de Defensa, TIC y Justicia crear una comisión de expertos del más alto nivel para recomendar qué debe hacer el país con el fin de fortalecer la seguridad y la ciberdefensa.

Por ello se han efectuado encuentros y talleres con especialistas nacionales e internacionales con el fin de hacer el diagnóstico y trazar la hoja de ruta en este campo, explicó la viceministra María Isabel Mejía en su introducción al panel "¿Cómo avanza Colombia en su estrategia?".

Lo primero que hicieron, dijo la funcionaria, fue un taller de expertos del Gobierno, la industria TIC, los sectores privado y financiero, las empresas con infraestructuras críticas, los abogados y la academia, y se presentó el diagnóstico con las prioridades. Este material fue empleado en otra consulta con expertos de ocho países que dieron unas recomendaciones en las que se está trabajando. El estudio lo organizaron en cuatro temas: gobernabilidad e institucionalidad, fortalecimiento de capacidades, cooperación nacional e internacional y marco jurídico y normativo.

Resultaron, entre otras, estas sugerencias:



Cuadro presentado por la viceministra María Isabel Mejía.

Gobernabilidad e institucionalidad

- Crear la Agencia de Seguridad Cibernética que dependa, preferiblemente, de la Presidencia y coordine las diferentes instancias encargadas de ciberseguridad y ciberdefensa en el país. De ella dependería directamente el ColCERT (Centro de Respuesta a Emergencias Cibernéticas).
- Establecer un mecanismo formal y permanente para trabajar conjuntamente el Gobierno, la academia, el sector privado y la sociedad civil. La política que rige es el Conpes del 2011 y su plan de acción tiene vigencia hasta este año (2014).
- Enfocarse en las infraestructuras críticas. Detectar cuáles son y determinar cómo defenderlas.
- Conformar una visión global y compartida entre todos los actores.
- Crear fiscalías especializadas en ciberdelito y nombrar un coordinador de la política internacional en ciberseguridad.

Fortalecimiento de capacidades

- Conformar un ecosistema con centros de pensamiento (*Think tanks)* para reflexionar estructuradamente en temas de seguridad y ciberdefensa y definir políticas y estrategias a largo plazo.
- Crear centros de excelencia para formar personas y un centro de innovación.
- Fortalecer la industria de información y armar un clúster de las empresas colombianas, productos o servicios especializados en seguridad cibernética.
- Cambiar de un enfoque basado en amenazas a uno global basado en riesgos. Y abrir centros sectoriales de respuesta

a incidentes de seguridad informática. Para evaluar riegos y hacer seguimiento, abrir un observatorio estratégico del cibercrimen y del *malway*.
- Apoyar a las mipymes.
- Mejorar los hardware, los software, los laboratorios, etcétera.

Cooperación nacional e internacional

- En el ámbito nacional, que todas las entidades públicas y privadas hagan un reporte obligatorio de incidentes. Tener una red de alertas. Hacer jornadas de actualización tecnológica para retroalimentar a los proveedores.
- En el plano internacional, tener una agenda estratégica de cooperación, un intercambio de conocimientos y experiencia permanente con otros países, pertenecer a la red 724 de Interpol y facilitar el intercambio de datos.

El marco jurídico

- Adherirnos al Convenio de Budapest, para lo cual ya el Gobierno adelanta gestiones.
- Armonizar la legislación en materia de inteligencia con la legislación sobre privacidad.

Colombia vive una revolución digital

En el panel, la Viceministra entregó los siguientes datos:

› Existen 8.8 millones de conexiones a internet; al principio del Gobierno había 2.2 millones.
› Las mipymes conectadas han crecido 767 %: pasaron de 7 % en el 2010 a 60 % en el 2013.
› Los hogares conectados eran el 17 % en el 2010 y actualmente son el 44 %.
› La meta para este año es llegar al 50 % de los hogares conectados.
› Más de 1900 trámites con el Estado pueden hacerse en línea.
› El 59 % de los ciudadanos y el 79 % de las empresas interactúan con el Estado a través de medios electrónicos.

> “Los bancos pueden diseñar la página más segura, pero si el usuario es descuidado, los esfuerzos se pierden”.
>
> **Gina Alejandra Pardo, directora de operaciones bancarias.**

María Isabel Mejía, viceministra TSI, explicó que Colombia adelanta varios proyectos encaminados a la seguridad y la ciberdefensa.

- Promulgar leyes orientadas a la conservación de la evidencia física y hacer que los proveedores de servicios de internet guarden la información por cierto tiempo.
- Construir una visión global y compartida, privada, pública y académica, para trazar una política que debe convertirse en otro documento Conpes.

Hablan diversos sectores

El moderador, José Carlos García, de *El Tiempo*, interrogó sobre cómo va la ciberseguridad en sus áreas.

Gina Alejandra Pardo, directora de operaciones bancarias: Cada vez más hogares y mipymes están conectados a internet y a los sistemas financieros. Los bancos invierten millones de dólares en la seguridad para que sus redes no vayan a ser penetradas. Sin embargo, hay que diseñar productos que sean seguros pero usables.

Los bancos pueden diseñar la página más segura, pero si el usuario es descuidado con las claves, no tiene software legal o antivirus, los esfuerzos se pierden en el camino.

Juliana García, directora de Seguridad Pública e Infraestructura del Ministerio de Defensa: La Policía tiene muchos programas de protección a los niños contra la pornografía infantil, de uso responsable de internet y de las tecnologías de la información.

Siguiendo los lineamientos del Conpes 2011, el sector defensa está organizado de la siguiente manera: el ColCERT (Centro de Respuesta a Emergencias Cibernéticas), el Comando Conjunto Cibernético (CCOC) que hace parte del Comando General de las Fuerzas Militares, y el Centro Cibernético Policial (CCP), encargado de la lucha contra el cibercrimen.

Yezid Donoso, director de la Maestría en Seguridad de la Información (MESI) de la Universidad de los Andes: La conciencia que tiene la persona es uno de los puntos críticos porque la seguridad la hacemos todos. Si manejo el esquema de seguridad, puedo evitar, y si hay conciencia, puedo prevenir. Hay que sensibilizar a la gente, socializar los conceptos y ahí comenzamos a formar un armazón más robusto y verdadero en una sociedad que vive el tema. Sabemos hacer las cosas pero no necesariamente somos conscientes de los riesgos. ■