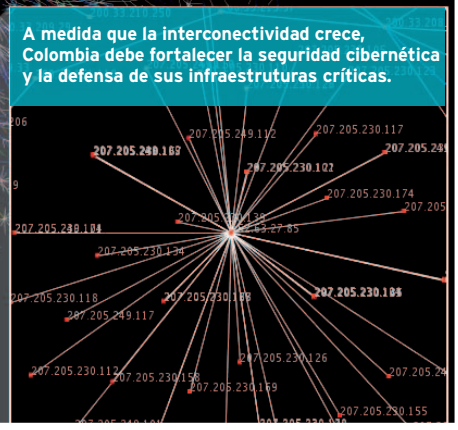
El peligro existe y va al alza

Para contribuir a crear una política de seguridad cibernética, la Universidad de los Andes y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), con el apoyo de MinTIC, organizaron este encuentro con más de 30 expertos de distintos sectores, 5 paneles y 11 talleres. Se estudiaron el contexto mundial y colombiano, el desarrollo de la ciberseguridad y la ciberdefensa, las experiencias, los retos, las oportunidades y la relación con los ciudadanos y los derechos humanos.



A medida que la interconectividad crece, Colombia debe fortalecer la seguridad cibernética y la defensa de sus infraestruturas críticas.

Foto: Internet map 1024. By The Opte Project [CC-BY-2.5 (http://creativecommons.org/licenses/by/2.5)], via Wikimedia Commons

En el periodo de Navidad del 2012, se perpetró uno de los grandes ataques cibernéticos a las tiendas Target, de supermercados y por departamentos de Estados Unidos, y sus propietarios debieron aceptar que les habían robado decenas de millones de datos de sus clientes, incluyendo números de tarjetas de crédito. Antes de este suceso, empresas como American Express, Visa, Master Card, Google y Yahoo también habían perdido información por ataques similares.

Estos datos de la revista *Forbes* muestran la magnitud del ciberdelito, señaló Eduardo Behrentz, decano de la Facultad Ingeniería de Los Andes, al instalar el "Foro seguridad y defensa cibernética: una estrategia de país", efectuado el 27 y el 28 de mayo del 2014. Y agregó que el Departamento de Seguridad Nacional de Estados Unidos tiene cifras impresionantes: en el 2007, cuando fue lanzado Twitter, hubo 12.000 ataques cibernéticos a la red; en el 2009 la cifra se duplicó y en el 2012 se cuadriplicó. "Estos datos muestran que la amenaza existe y va al alza", puntualizó.

El encuentro hizo parte de los Foros ISIS, organizados por el Departamento de Ingeniería de Sistemas y Computación (DISC) de Los Andes. En él, representantes de la academia, el Gobierno, las empresas y la sociedad civil compartieron puntos de vista y reflexionaron para construir un marco de trabajo conjunto que permita crear una visión de largo plazo sobre la seguridad y la defensa cibernética en el país.

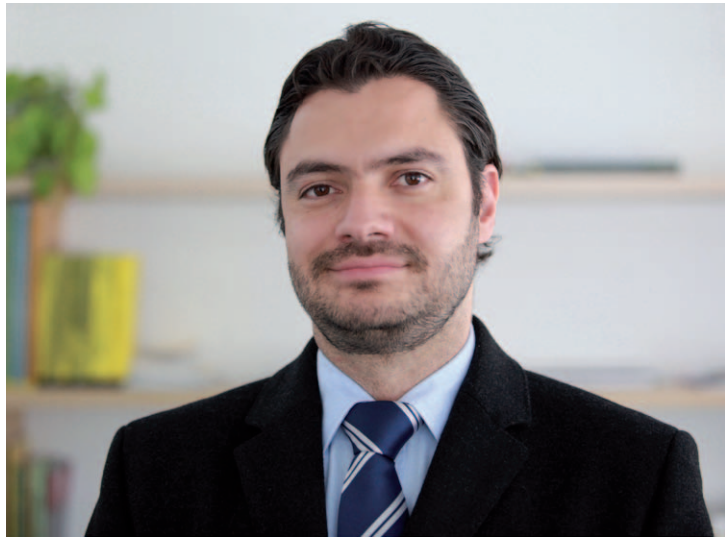
Expertos como Erick Erez Kreiner, de Israel, marcaron la diferencia entre los conceptos de ciberseguridad y ciberdefensa. La primera corresponde a los subdominios que conforman el ciberespacio de un país como las fuerzas del orden, las infraestructuras críticas, las empresas y el público en general, mientras que la ciberdefensa concierne al Estado y al ciberespacio.

El trabajo debe seguir. "Este es un recorrido en el tiempo y es continuo. No podemos decir que en un momento vamos a encontrar el estado ideal de la seguridad, eso significaría bajar la guardia. Si los riesgos son dinámicos, nuestro reaccionar tiene que ser dinámico", expresó Yezid Donoso, director de la Maestría en Seguridad de la Información (MESI) de la Universidad de los Andes.

Y este foro quiere destacar, agregó el profesor Donoso, que "la seguridad es estrategia, no es solamente táctica y operativa. Tiene que existir en todos los niveles de las organizaciones, el Gobierno y la academia, y, por otro lado, es un problema de país".

El evento, precisamente, respondió al interés del Gobierno de crear una alta comisión para estudiar la estrategia de seguridad cibernética. Colombia ha superado distintas etapas para darles a la ciberseguridad y la ciberdefensa un lugar preponderante y se estudia la creación de una gran agencia que coordine a nivel nacional y a largo plazo a todos los organismos especializados en esta materia.

> "Este es un recorrido en el tiempo y es continuo. No podemos decir que en un momento vamos a encontrar el estado ideal de la seguridad, eso significaría bajar la guardia. Si los riesgos son dinámicos, nuestro reaccionar tiene que ser dinámico".
>
> **Yezid Donoso**



El encuentro fue instalado por Eduardo Behrentz, decano de la Facultad de Ingeniería.

Para ello, es importante contar con un espacio donde los diferentes sectores sociales puedan hacer recomendaciones. Alberto Samuel Yohai, presidente de la CCIT, agregó que se requiere una alianza estratégica entre el sector privado, la academia y el Gobierno. "Y lo más importante es generar una conciencia y ser responsables de cuidar nuestras vidas digitales".

En la instalación del evento, además participaron Milena Ortiz, secretaria general del Ministerio de Justicia; María Isabel Mejía, viceministra de Tecnologías y Sistemas de la Información (TSI) y Javier Fernández Leal, director de la Escuela Superior de Guerra.

Academia, Estado y empresas

Desde el punto de vista del Gobierno, María Isabel Mejía, viceministra TSI, señaló que han trabajado desde el 2006 para que todos los trámites en línea sean seguros y generen confianza en los ciudadanos. "El 53 % de los colombianos emplean medios electrónicos con el Estado, pero queremos crecer y contamos con el programa En TIC Confío que promueve el uso responsable y seguro de la tecnología" (ver pág. 37).

Javier Fernández Leal, director de la Escuela Superior de Guerra, apoyó estas ideas y agregó que "los temas estratégicos ya no son solo de los militares".

Las naciones se unen contra el cibercrimen

"Cuando se comete un delito en Colombia, los servidores pueden estar en Argentina, Estados Unidos o en cualquier parte del mundo y tenemos que estar preparados para enfrentarlos con una visión global", expresó Adrián Acosta, de Interpol, en la introducción al panel "Panorama mundial en materia de ciberseguridad y ciberdefensa". Agregó que varios países están tratando de unirse contra el cibercrimen porque han tomado conciencia sobre los peligros, al tiempo que están actualizando sus legislaciones.

Adrián Acosta está encargado del área postecnológica para América de Interpol, una organización que asumió la ciberseguridad como prioridad ante el incremento de *hackers* y delitos en la red. Y por otro lado, organizaciones internacionales como la OEA y Naciones Unidas avanzan en el manejo de este nuevo panorama.

Los atacantes de diferentes países se unen para cometer los delitos. Y para combatirlos hay que tener un estándar mundial en lo que respecta al cibercrimen, explicó el conferencista. Una manera de lograrlo es a través del Convenio de Budapest, el cual

permite esta paridad legislativa y propicia la cooperación y la interacción policial, fiscal y en otros ámbitos. Colombia está dando los pasos para suscribir ese tratado.

"Hay países que tienen más experiencia y más conocimiento. Y es importante compartir la capacitación, la experiencia y su conocimiento. Hace unos años, decíamos: vamos a formar al policía y al militar, hoy tenemos que instruir a toda la ciudadanía para que conozca lo que puede pasar en internet", señaló Acosta.

¿Qué está sucediendo en el mundo?

No solo aumenta la cantidad de software malicioso para atacar instituciones específicas del gobierno o financieras, sino que se están desarrollando programas más sofisticados que pueden ser adquiridos a precios cómodos y manejados por principiantes, explicó el especialista, John Kemon, de Macafee, en el panel sobre el panorama mundial, moderado por la viceministra TSI.

También se han incrementado los ataques a través de las redes sociales, agregó Kemon: "Se crean cuentas falsas de Facebook para ganar la confianza de trabajadores gubernamentales y así obtener información y, posiblemente, enviarles un vínculo embebido que los lleve a un sitio web". Además, advirtió: "Si el acceso a las redes sociales no se hace solo en la vivienda y alguien revisa su Facebook y hace clic en un vínculo malicioso, es un riesgo para la red interna de la organización donde está".

Yezid Donoso, director de la Maestría en Seguridad de la Información de Uniandes; Milena Ortiz, secretaria general del Ministerio de Justicia; Javier Fernández Leal, director de la Escuela Superior de Guerra; María Isabel Mejía, viceministra de TSI y Alberto Samuel Yohai, presidente Cámara Colombiana de Informática y Telecomunicaciones.

> "Se requiere una alianza estratégica entre el sector privado, la academia y el Gobierno. Y lo más importante es generar una conciencia y ser responsables de cuidar nuestras vidas digitales"
>
> **Alberto Samuel Yohai**

En el panel sobre el panorama mundial de la seguridad y la defensa cibernética, participaron John Kemon de McAfee, Systems Engineer, North America Federal Department; Adrián Acosta, de Interpol; Erez Kreiner, de Israeli National Cyber Bureau, y María Isabel Mejía, viceministra TSI.

Por su parte Erez Kreiner señaló que Colombia adelanta iniciativas para tener un ciberespacio ciberseguro, como suscribir el Convenio de Budapest y actualizar su legislación, pero la segunda etapa debe ser capturar a los criminales, combatir a los delincuentes y prevenir el delito.

Infraestructuras críticas

Con respecto a este tema, la viceministra Mejía preguntó: ¿Cómo se están preparando los países para protegerlas?

Erez Kreiner respondió: "Tuve la experiencia, hace más de 12 años, cuando el Gobierno de Israel me encomendó establecer cuáles eran las infraestructuras críticas del país, y cuando uno las define, concreta lo qué está en el corazón de la seguridad nacional, porque estas combinan la defensa, la economía y la vida social. Después de cuatro meses, llegamos a la lista y precisamos los criterios de qué es una infraestructura crítica. Enfocarnos nos permitió invertir en los lugares correctos porque hay que emplear eficientemente los presupuestos". ■