Posconflicto, retos y oportunidades para la seguridad digital

En junio del 2016, Foros ISIS reunió a académicos, empresarios y representantes del Gobierno para hablar sobre los retos y oportunidades que surgen en una eventual reinserción de la guerrilla. Se habló de cómo proteger los datos de quienes dejen las armas y de las víctimas, de manejar la información digital de forma segura y de generar espacios para las empresas nacionales de tecnología.

Foto: Natalia Fernanda Madrid Vidales

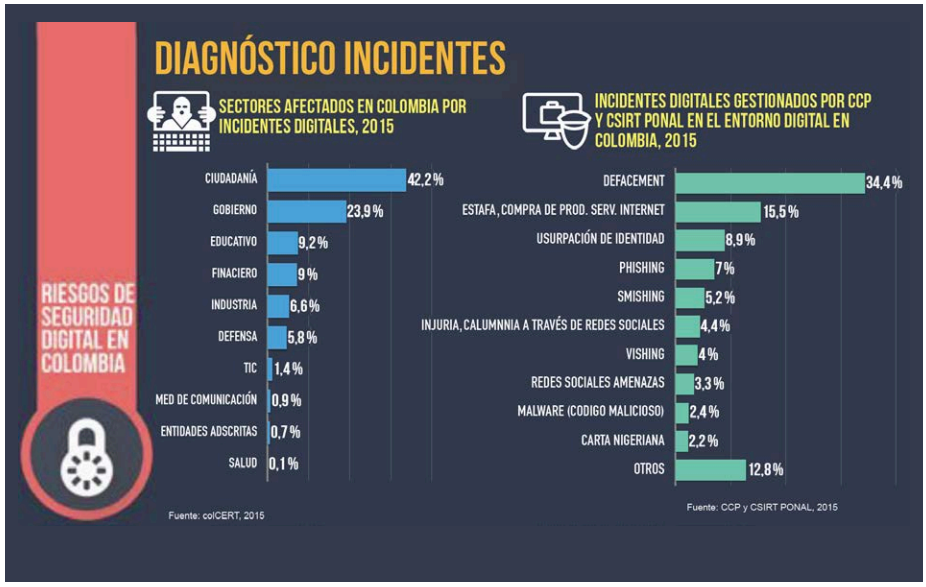
El auditorio del edificio Mario Laserna fue el escenario de las plenarias que se desarrollaron durante la mañana. Por la tarde hubo sesiones simultáneas para tratar aspectos puntuales de la seguridad informática.

Con 6,9 millones de desplazados, Colombia ocupa el primer deshonroso lugar del mundo en ese aspecto, según la Agencia de las Naciones Unidas para los Refugiados. Y en julio del 2016 había poco más de 8 millones de víctimas, 7,7 millones de las cuales dijeron que la causa era el conflicto armado, de acuerdo con el Registro Único Nacional de Víctimas. Una triste realidad que ya supera a países como Siria, inmerso en una guerra civil.

La confrontación armada en nuestro país tiene más de medio siglo, una condición que lo hace único. En un eventual posconflicto surgen retos y oportunidades para garantizar la seguridad de la información digital de los combatientes que se desmovilicen y de los millones de víctimas.

¿Qué deben hacer el Estado, el sector privado, la academia y los ciudadanos para facilitar la reinserción de los guerrilleros y el retorno de los desplazados a sus tierras?, ¿para minimizar los riesgos de fugas de datos con la consecuente estigmatización de esas personas? y ¿para impulsar el desarrollo y apropiación de tecnología para resolver los retos planteados?

> **"La transición hacia una economía digital incrementa los riesgos en seguridad informática porque hay más incertidumbres, amenazas y vulnerabilidades".**
>
> María Isabel Mejía



María Isabel Mejía, entonces viceministra TSI, presentó cifras de las amenazas que se ciernen sobre la sociedad. Se basó en reportes de diversas agencias de la Policía Nacional que combaten estos delitos.

Estos temas fueron tratados el 22 de junio del 2016 en el Segundo Foro Nacional de Seguridad de TI "Desafíos y oportunidades de la seguridad de la información en la era del posconflicto". Este fue organizado por el Departamento de Ingeniería de Sistemas y Computación (DISC) de la Universidad de los Andes.

En el encuentro participaron María Isabel Mejía, entonces viceministra de Tecnologías y Sistemas de Información (TSI) del MinTIC; Luis Mauricio Vergara, especialista en soluciones de ciberseguridad para Latinoamérica de la compañía NEC; coronel Fredy Bautista, jefe de área del Centro Cibernético Policial; Jorge Bejarano, director de estándares y arquitecturas de TI del MinTIC, y otros expertos que estuvieron en un panel (ver pág. 9) y condujeron sesiones simultáneas sobre temas puntuales durante la tarde.

La viceministra Mejía habló de "La nueva Política Pública de Seguridad Digital: desafíos y oportunidades en el escenario de posconflicto". Centró su exposición en el Conpes 3854 del 2016 y destacó que Colombia tiene una situación única no solo por los factores ya mencionados del conflicto interno, sino porque su legislación ha tenido en cuenta los lineamientos de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre seguridad digital emitidos en el 2015. Estos se enmarcan en principios generales de gestión de riesgo, "un concepto que no se consideraba antes", y trascienden temas técnicos de ciberseguridad y ciberdefensa digital al incluir un componente de prosperidad económica y social.

La funcionaria señaló que Colombia expidió el Conpes 3701 sobre ciberseguridad y ciberdefensa con vigencia 2011-2014. En el 2014 se empezó a preparar uno nuevo para adaptar el marco jurídico e institucional a la transición hacia una economía digital que se está dando en el mundo. La razón es que esta incrementa los riesgos en seguridad informática porque hay más incertidumbres, amenazas y vulnerabilidades en el entorno digital (ver "Diagnóstico de incidentes", pág. 6 y "Diagnóstico de denuncias", pág. 7).

Con ese fin se constituyeron mesas de trabajo con expertos nacionales e internacionales y se consultaron políticas adoptadas por diversos países desde el 2000. Al mismo tiempo se consideraron las recomendaciones de buenas prácticas de organismos internacionales como la Organización de Estados Americanos (OEA), la Unión Internacional de Telecomunicaciones (UIT), la Organización del Tratado del Atlántico Norte (OTAN) y el Information Technology Industry Council (ITI), que agrupa empresas de TI en el mundo.

Ejes y estrategias de seguridad digital

María Isabel Mejía enfatizó que la nueva política se basa en la salvaguarda de los derechos humanos y para ejecutarla se asignaron 85.000 millones de pesos, 48 % de los cuales los aporta MinTIC, 47 % el Ministerio de Defensa y el resto otras entidades estatales.

Los ejes de esa política los resumió así:

1. Gestión de riesgos, para lo cual se debe establecer un marco institucional que especifique cuáles entidades coordinarán el Conpes y también hacer ajustes legales y regulatorios.
2. Liderazgo de alto nivel en el Gobierno. Es necesario crear un tanque de pensamiento que diseñe, haga seguimiento y evalúe las políticas. Así mismo, se adelantará un estudio sobre el impacto de los delitos y crímenes del entorno digital mediante un convenio con la OEA.
3. Enfoque multidimensional que contemple aspectos técnicos, jurídicos, sociales y económicos relacionados con su implementación. Esto supone mejorar los controles, los procedimientos y los procesos para que se dé el intercambio de información entre entidades como la Unidad de Restitución de Tierras, la Superintendencia de Notariado y Registro, el Instituto Geográfico Agustín Codazzi, el MinTIC, el Incoder, el Consejo Superior de la Judicatura, la Fiscalía y la Registraduría Nacional del Estado Civil.
4. Responsabilidad compartida entre el Estado, los ciudadanos, las empresas y la academia, en un enfoque incluyente y colaborativo.
5. Generación de confianza y educación. Se asignó al Ministerio de Educación Nacional la tarea de crear conciencia sobre la seguridad digital desde la primaria. A su vez, el MinTIC desarrolla proyectos y campañas de apropiación, socialización y concienciación como En TIC Confío.
6. Fortalecer la seguridad de los individuos y del Estado, luchar contra el cibercrimen y la ciberdelincuencia, fortalecer la defensa y la soberanía nacionales mediante cooperación nacional e internacional e impulsar la transferencia e intercambio de conocimiento.

Retos y oportunidades

Al final de la mañana y durante la tarde, el foro se dividió en sesiones con enfoques particulares: Gobierno, academia, ciudadanos e industria. En una de estas sesiones Luis Mauricio Vergara, experto en soluciones de ciberseguridad de NEC, habló de los "Desafíos del ecosistema digital en la era del posconflicto" y señaló los siguientes retos:

1. Protección de datos personales. Colombia cuenta con la Ley 1266 del 2008, o *habeas data* en el sector financiero, y la Ley 1581 del 2012, que regula los datos de los ciudadanos del común. Pero ¿cómo se tratarían los datos de los reinsertados de las Farc y los de los miles de desplazados para preservar su integridad y seguridad? ¿Se albergarían en bases de datos distintas como hicieron en El Salvador y Camboya, países que vivieron conflictos internos? ¿Se incluirían en la base general de la Registraduría, pero con una marcación especial? ¿Habría nueva legislación?

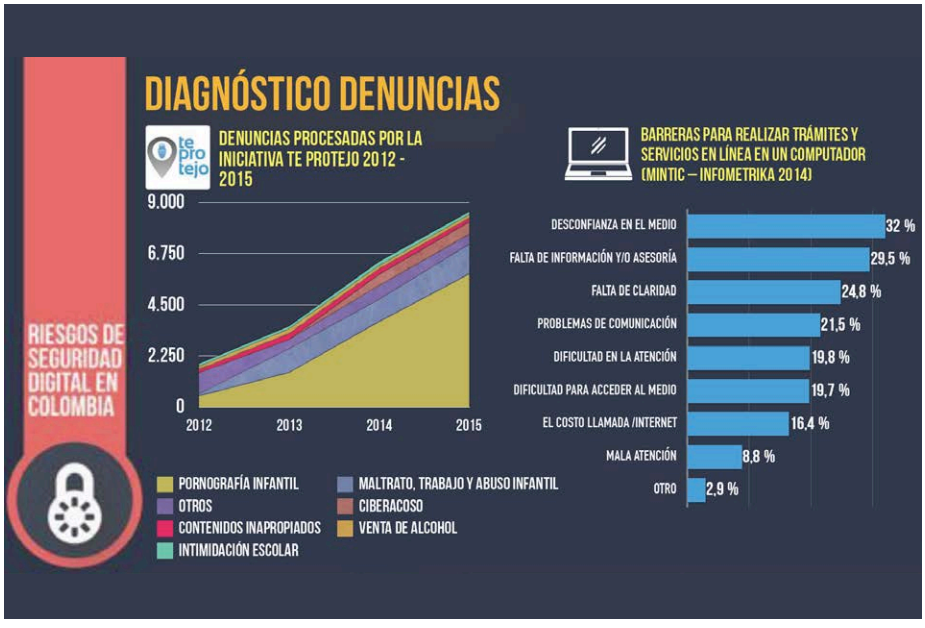
   Vergara formuló las preguntas porque hay riesgos como la fuga de información que podría ser aprovechada por las bandas criminales en dos sentidos. Por un lado, sería posible suplantar la

La inversión, un imperativo

Luis Mauricio Vergara habló con revista Foros ISIS acerca de qué tan preparada está Colombia para proteger los datos de los reinsertados y de las víctimas y de cómo puede ayudar la tecnología en el posconflicto.

A su juicio, es indispensable poner estos temas sobre la mesa, pues en términos de ataques y fraudes cibernéticos, la cultura de muchas organizaciones colombianas es reactiva y no proactiva, es decir, actúan o invierten en seguridad cuando sus sistemas ya han sido vulnerados.

Para el experto, es necesario que las empresas inviertan en tecnología de seguridad para los sistemas en los que se alojarán las bases de datos de las víctimas y de los reinsertados. El Gobierno puede regular las condiciones de uso de esta información, tal como ha hecho la Superintendencia Financiera con el sector bancario al exigirle implementar mecanismos para preservar la confidencialidad e integridad de la información.



Fuente: Exposición de María Isabel Mejía, entonces viceministra de Tecnologías y Sistemas de Información (TSI).

Foto: Natalia Fernanda Madrid Vidales

Conferencistas del segundo foro de seguridad organizado por el DISC.

> **"La fuga de información podría ser aprovechada por las bandas criminales para suplantar la identidad de quienes reciban subsidios del Estado o para revelar el pasado de resintertados y víctimas y generar rechazo y discriminación".**
>
> Luis Mauricio Vergara

identidad de los reinsertardos para cobrar los subsidios que les otorgaría el Gobierno o adulterar los datos de las víctimas para impedirles recuperar sus tierras cuando quieran regresar a sus orígenes; también podrían revelar su pasado lo que generaría discriminación. Por el otro, esas organizaciones delincuenciales les contactarían a quienes están desencantados para invitarlos a delinquir.

2. Para gestionar esos riesgos, es necesario establecer pautas para clasificar la información, determinar cuál es sensible, con el fin de definir quién tendría acceso a ella y con cuáles privilegios. También se deberían definir protocolos para tener acceso a información protegida, por ejemplo ¿cómo se consultarían los antecedentes judiciales, crediticios, académicos y laborales de los reinsertados que aspiraran a un trabajo?
3. Se requeriría contar con sistemas fuertes de autenticación para evitar suplantaciones, así como fortalecer las regulaciones y controles para compartir información entre las instituciones que se relacionan con los reinsertados, como entes de control, prestadores de servicios, agencias estatales y banca.
4. Habría que educar a los reinsertados para generar conciencia sobre la importancia de la seguridad de la información digital. Las organizaciones invierten dinero en capacitación y, sin embargo, cada vez que salen los listados de las peores contraseñas del mundo, aparecen las mismas: 1234, *password,* ABC y otras similares. Es probable que los excombatientes no hayan tenido mucha relación con los computadores y no solo habría que pedirles que usaran contraseñas robustas, sino explicarles qué significan esos conceptos.
5. Cómo combinar los derechos a la privacidad y a la libre expresión en redes sociales. ¿Qué pasaría si hubiera fuga de información y esta se hiciera pública? ¿Cómo evitar que la imagen de una persona sea expuesta, se vuelva viral en segundos, sea discriminada y se sienta rechazada? Esta tarea no le compete solo al Gobierno, sino que necesita ayuda del sector privado y de la academia para definir buenas prácticas y procedimientos.

> **"La nueva política de seguridad digital se basa en la salvaguarda de los derechos humanos. Para ejecutarla se asignaron 85.000 millones de pesos".**
>
> María Isabel Mejía

En la sesión del Gobierno, el coronel Erich Siegert, del Ministerio de Defensa, presentó el trabajo que está adelantando el Comando Conjunto Cibernético, con la colaboración de diversas entidades públicas y privadas, en la identificación de la infraestructura crítica cibernética nacional. Esta tarea responde a la necesidad de proteger infraestructura cibernética que soporta los servicios esenciales ofrecidos a la población colombiana. En la segunda parte, el teniente John Albeiro Guevara, de la Policía Nacional, resaltó la necesidad de asumir los retos planteados por la seguridad digital como una tarea comunitaria, no solo del Gobierno, y dijo que todos debemos contribuir.

En la sesión de la academia, el profesor Martín Ochoa llamó la atención sobre la tendencia creciente en la interconexión de infraestructuras críticas a internet y la relevancia del papel de los académicos para entender mejor la situación y proponer soluciones con fundamentos sólidos. Más tarde, la coronel Martha Sánchez, de la Escuela Superior de Guerra, indicó que los programas educativos deberían transformarse para responder al posconflicto y a nuevos desafíos. Dichas transformaciones requerirían una estrategia que considerara las normas establecidas e incluyera un alto grado de innovación y cooperación con otras instituciones. En la segunda parte de la sesión, Manuel Sánchez Rubio, invitado de la Escuela de Telemática de la Policía Nacional, hizo énfasis en la necesidad de aprovechar el talento de los estudiantes para abordar problemas y plantear soluciones novedosas y prácticas.

En las sesiones de ciudadanos e industria participaron Adriana Bueno, de Oracle; Wilmer Prieto, de Foundstone; Luis Carlos Sanmartín, de Security Zone, y Robin José Salcedo, de Identian. Entre los temas que tocaron están las ventajas de la convergencia de tecnologías recientes como *cloud*, IoT, móviles y *big data* para ofrecer servicios innovadores, pero al mismo tiempo la necesidad de incorporar componentes de seguridad para garantizar la protección de la información de los clientes de un servicio. También mencionaron la importancia del desarrollo de competencias ciudadanas en seguridad digital y de educar a los más jóvenes.

Todos los expertos que participaron en el foro coincidieron en que se espera que el Gobierno, la academia y las empresas colombianas de tecnología desarrollen nuevas propuestas o personalicen las existentes para responder de la manera más apropiada a los retos planteados. Esta situación genera una oportunidad única de desarrollo que Colombia debe aprovechar. ■

La tecnología, gran aliada de la paz

Expertos en ciberseguridad y ciberdefensa participaron en un panel sobre los desafíos y las oportunidades para garantizar la protección de la información en el eventual posconflicto mediante herramientas informáticas.

La tecnología es un aliado de primer orden para crear una arquitectura unificada que permitiría a las entidades que manejen datos de los reinsertados y de las víctimas dar acceso a estos datos de forma segura. Pero también es un instrumento empleado para difundir mentiras, discriminar o crear pánico, de suerte que es necesario crear conciencia para que se use con responsabilidad y contribuya a consolidar la paz en el eventual posconflicto. Así lo resaltó Sandra Peña, jefe de redacción de *Computerworld,* quien moderó el panel de expertos.

Los participantes fueron Jean Marie William Chenou, profesor de la Maestría en Construcción de Paz de Los Andes; Luis Mauricio Vergara, especialista en soluciones de ciberseguridad para Latinoamérica de la compañía NEC; Jorge Bejarano, director de estándares y arquitectura de TI del Ministerio de Tecnologías de Información y Comunicaciones; coronel Fredy Bautista, jefe de área del Centro Cibernético Policial; coronel Erich Siegert Cerezo, comandante del Comando Conjunto Cibernético (CCOC), y Sandra Rueda, profesora del