Ciberseguridad, nuevo **reto vital** para el país

Las organizaciones criminales cuentan con inmensos recursos que les permiten corromper, infiltrar y ocasionar grandes daños a los sistemas informáticos, por lo cual es esencial proteger los datos.

Gobierno, banca y empresas son cada vez más blanco de los ciberdelincuentes: En el mundo, los robos les cuestan 114.000 millones de dólares, según el fabricante de antivirus Norton, y los ataques han crecido 44 %. Al mismo tiempo, un informe de Naciones Unidas indica que dos terceras partes de los ataques al ciberespacio en el 2011 estaban asociados a crímenes relacionados con elementos patrimoniales.

Lo anterior significa que la seguridad cibernética no es un asunto menor y que, como dijo el profesor Yezid Donoso, en la presentación 1er Foro Nacional de Seguridad en TI, "no es un problema exclusivamente financiero, del Gobierno, de la academia. Es un problema de país. Eso significa profesión, continuidad, sostenibilidad y supervivencia de los negocios de los diferentes sectores de una nación".

Este fue el primer foro ISIS dedicado al tema y se centró en el impacto de la seguridad en las estrategias de las empresas. Se llevó a cabo el 21 de febrero pasado en Los Andes y tuvo como conferencista principal a Luis Edmundo Suárez, director de la Unidad de Información y Análisis Financiero (UIAF) del Ministerio de Hacienda, que habló sobre "La seguridad cibernética en el centro de la problemática mundial". Por el Gobierno también participó Leonardo Huertas, asesor de Seguridad y Ciberdefensa del Ministerio de Defensa, con una exposición sobre cómo se está enfrentando la ciberdelincuencia en el país.

Luis Edmundo Suárez, director de la UIAF.

> "Es imposible luchar contra una amenaza de estas proporciones sin que el sector público y el privado trabajen de forma realmente coordinada".
>
> **Luis Edmundo Suárez.**

La visión estratégica por tipo de industria la dieron Germán Patiño, experto en seguridad, *sales manager* de NoLA Trusteer, por el sector de la banca, y Jahir Molina Zuleta, gerente de Operaciones Tecnológicas de Emtelco S.A., por telecomunicaciones.

Las estrategias de seguridad y la referencia a algunos casos en compañías estuvieron a cargo de Vicente Gozalbo, de IBM Security Solutions Tiger Team, Latam; Jesús Jiménez, director técnico de Seidor Colombia, y Guillermo Angarita Morris, de IQ Information Quality.

Amenazas y ciberespacio

Luis Edmundo Suárez, director de la UIAF, centró su exposición en la urgencia de proteger los datos de los ciberataques y enfatizó en que "no es posible desconectar la seguridad de la información del resto de las amenazas que se ciernen hoy y menos desligarla de su estrategia de negocio".

A su juicio es importante compartir la responsabilidad entre el sector público y privado del país porque "no existe una amenaza de una dimensión, un tamaño, un impacto tan fundamental contra la seguridad de la información, como la ciberamenaza. La globalización y la tecnología han cambiado nuestro mundo de forma vertiginosa y a veces sentimos que vamos un poco a la zaga".

Las dimensiones de seguridad

El término de seguridad como disciplina académica y científica es reciente, explicó Suárez. Antes de la II Guerra Mundial se refería a los Estados pero luego de la Guerra fría, el concepto se hizo más complejo. En los 80 una gran corriente señalaba que el concepto no se refería solamente a lo militar. Incluso Barry Buzan, representante de la Escuela de Copenhague, publicó

> Debemos tomar políticas preventivas y no reactivas frente a los riesgos de seguridad. Sabemos que estamos expuestos a ataques, no esperemos a que nos sucedan para poder reaccionar". **Jesús Jiménez.**

el libro hito G*ente, Estados y miedo*, en el que afirma que al lado de lo militar, de la protección de las fronteras y de los ejércitos, están las dimensiones política, del medio ambiente, sociológica y económica.

Desde esa esfera económica, Suárez explicó que el lavado de activos afecta la seguridad y la defensa nacional: "Uno puede reconocer diferentes organizaciones criminales en Colombia —bandas de narcotráfico, corrupción, generación de ciberamenaza—, pero la intención de obtener lucro ilícito es lo que les da existencia y fortaleza. Ese es el elemento transversal de todos".

Un informe de la Oficina contra la Droga y el Delito de las Naciones Unidas del 2011 estima que, fruto del crimen, en el mundo se mueven US$ 2,1 trillones, que equivalen a todo el PIB de Brasil o de Italia en un año. De ellos, 1,6 trillones son lavados y se reinvierten en el sistema económico, y medio trillón se usa para seguir perpetrando el ilícito. La posibilidad de corrupción, de infiltración, de daño que puede efectuar es enorme. Por eso la protección de la información es absolutamente crítica y esencial pero es insuficiente. Necesitamos ser más proactivos y cerrar la posibilidad a los delincuentes".

La tasa mundial promedio de interceptación de estos recursos es inferior al 1 % y se sitúa en cerca del 0,20 %, es decir que de cada 100 pesos solo capturan 20 centavos. Esto significa que "difícilmente vamos a detener el delito".

Algo similar sucede, a juicio del abogado Suárez, con los grupos insurgentes y terroristas en el país: "Colombia lleva 50 años combatiéndolos y no hemos logrado unos resultados efectivos por muchas causas, pero una de las fundamentales es que estamos atacando parte de las estructuras criminales pero no su parte esencial. Hemos afectado los nodos de la red pero no la red en sí misma. Mientras no les toquemos estos recursos, las organizaciones criminales no van a disminuir".

¿Qué se está haciendo? En el mundo, el sistema antilavado nació en 1989, con la creación del grupo de Acción Financiera Internacional fundamentado en tres pilares: Criminalización (en los ochenta no existían como delitos ni el narcotráfico ni el lavado), Responsabilidad Compartida y Centralización de la Información con Unidades de Inteligencia Financiera en distintos países (existen 143 unidades).

La seguridad TI es un requerimiento cada vez más grande porque el avance científico es vertiginoso. "Se necesitaron 46 años para que el 25 % de Estados Unidos masificara la electricidad, se requirieron 35 años para el teléfono, 31 para el radio y hoy estamos en menos de 5 y 4 años para las nuevas tecnologías", señaló Luis Edmundo Suárez.

Eso genera un desafío gigantesco: "Como empresas tenemos que estar segundo a segundo mirando qué está pasando, para que la competencia no nos deje atrás, para que la información esté totalmente protegida".

A su turno, los demás conferencistas reiteraron que la seguridad es compromiso del sector público y privado y de los usuarios. Con respecto a la responsabilidad en las empresas, Jahir Molina, de Emtelco, complementó: "No es un asunto solamente

El phishing, o robo de identidad, es una modalidad más elaborada de delito.

de la parte de tecnología. En una arquitectura de seguridad, siempre debemos involucrar las áreas críticas: la financiera, la de contabilidad, la de recursos humanos".

Y sobre su manejo, Germán Patiño, experto en seguridad en la banca, anotó: "No debemos pensar en el pasado para proteger el futuro. Todo lo que sabemos que funciona para los negocios de hoy, no funcionará para los de mañana" (ver En cinco años cada cliente va a usar banca móvil pág. 10).

De los virus al *phishing*

Jahir Molina hizo un recuento de los ataques a las telecomunicaciones, a las redes y a la industria desde los años setenta cuando proliferó el clásico virus. Explicó que luego apareció la moda de romper un sitio web; después, los códigos maliciosos como *Melissa*; del 2003 a 2005, los gusanos avanzados y troyanos, como *I Love You*. En el 2005, surgió el más sofisticado: el *phishing* o robo de identidad (ver cuadro. Tipo de ataques a las redes).

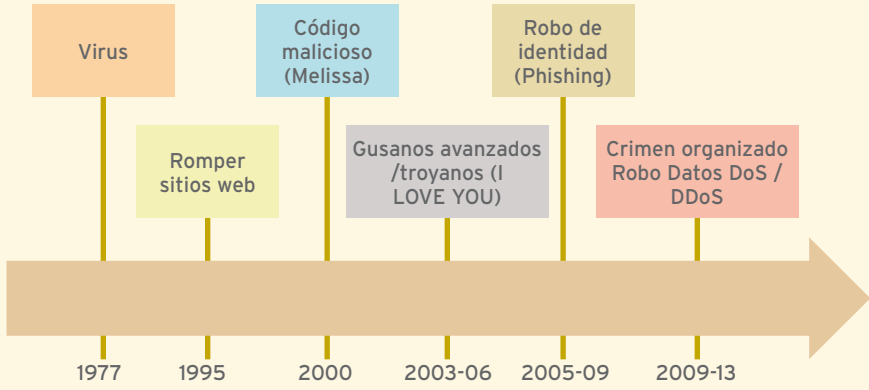
"A partir del 2009 —anotó el ingeniero de sistemas Molina—, el crimen organizado ha tenido como función el robo de datos y dejar los servicios por fuera de nuestra red para tener un control y, muchas veces, desde nuestra red, dirigir ataques hacia otras redes y otros sectores".

Al comparar los ataques del 2000 con los actuales, Molina señaló:

- Antes estaban enfocados a la infraestructura y buscaban penetrar el servidor; hoy quieren la interface del usuario, buscan los datos importantes.

Jahir Molina, de Emtelco.

Tipos de ataques a las redes



> "Uno de los mayores retos es como integrar usuarios, accesos y aplicaciones".
>
> **Jahir Molina.**

- Los ataques estaban enfocados a la red, ahora a las aplicaciones.
- Los objetivos eran el reconocimiento y el ciberatacante dejaba su marca, hoy apuntan a obtener ganancias.
- Los modos de ataque eran amenazas genéricas (*click and attack*); en el 2013 son elaborados y planeados con una estrategia definida, con maquinarias especiales, a cargo de una organización con jerarquías y personas aparentemente normales.

"Controles bien pensados aumentan la seguridad"

A medida que crecen los negocios, aumentan los riesgos y se hace necesaria una mayor regulación. Vicente Gozalbo, de IBM, se refirió a los conflictos de intereses que se presentan cuando un Departamento Técnico debe implementar aplicaciones seguras y tiene la necesidad de proteger las bases de datos pero existe un director financiero que no ve esto como algo estratégico. "Hay una colisión de intereses —explicó—. Por eso tenemos que buscar un balance entre la seguridad efectiva y el costo de la misma. La protección cien por cien no existe. Hay que tener un presupuesto y un plan, pues con unos controles bien pensados las empresas son capaces de aumentarla sensiblemente".

Visión y arquitectura de seguridad

"La seguridad es un esfuerzo continuo; la política de seguridad es constante. Es imperativo abordar todas las vulnerabilidades de forma sistemática", señaló Jahir Molina. Las redes cada vez son más complejas y crecen a medida que las empresas ofrecen nuevos servicios. Es importante tener primero una política y socializarla con todos. Las aplicaciones deben ser diseñadas por adelantado, y hay que asumir la seguridad en la red de principio a fin. Uno de los mayores retos es cómo integrar usuarios, accesos y aplicaciones.

Con respecto a la visión y arquitectura de seguridad anotó:

- Para enmarcar la seguridad dentro de la visión de la compañía hay que definir una arquitectura de seguridad con unos componentes claros, específicos.

> La comunidad internacional y las convenciones de Naciones Unidas han identificado por lo menos tres grandes nuevas amenazas: narcotráfico (1988), organizaciones criminales transaccionales (2000) y corrupción (2003)". **Luis Edmundo Suárez.**

- Para hacer esa arquitectura debe preguntarse: ¿Qué voy a proteger y cómo? ¿Para qué? ¿Qué actividades hago en mi red?
- La arquitectura debe tener tres niveles de seguridad: la infraestructura, los servicios y las aplicaciones. Al asegurar la infraestructura se aseguran los otros dos.
- Hay que contemplar ocho medidas: Control de acceso, autenticaciones de los datos, no repudio, confidencialidad de datos, seguridad de las comunicaciones, integridad de los datos, disponibilidad y privacidad.
- La estrategia de seguridad se alinea con el resto de los procesos de la compañía con un sistema de gestión de seguridad de la información, basado en personas, procesos y tecnología.
- Es necesario incluir los datos sensibles en la organización de la información teniendo en cuenta los activos, la seguridad física y ambiental y el recurso humano, que es el eslabón más débil.
- Otro reto de control son los dispositivos inteligentes: televisión, computadoras, tabletas, teléfonos móviles.

Germán Patiño, *sales manager* de NoLA, Trusteer.

Jesús Jiménez, del Grupo Seidor.

Las normas en la industria de pagos

En 2011, los colombianos gastaron más de 3,5 billones de pesos con tarjetas de pago. En el país hay aproximadamente 18 millones de tarjetas débito y 11 millones de crédito y esta cifra está aumentando año a año entre el 10 y el 14 %.

En la industria de pagos existen normas internacionales, definidas por las marcas de las tarjetas de crédito, que buscan que las transacciones sean seguras, pues esa condición es la que habilita el desarrollo de nuevos servicios, el ingreso a más canales de ventas y el acceso a otros segmentos del mercado, explicó Guillermo Angarita Morris, gerente de IQ Information Quality, durante su exposición. Estos criterios involucran varios elementos como el hardware de los cajeros automáticos o los datáfonos, los cuales son regulados.

Esas normas definen requerimientos para los datos mismos, las aplicaciones, las bases de datos, los sistemas operativos, las comunicaciones y la seguridad física. Además, constituyen una definición de procesos para ser utilizados por las entidades participantes. Como beneficios están la disminución del fraude, la madurez y estandarización del proceso, la disminución de costos de migración a autoservicio y la estandarización de requerimientos a terceros.

La mentalidad empresarial ha cambiado y la seguridad es vista como un problema estratégico manejado desde la alta dirección de las compañías con una política específica, unos procesos y una arquitectura. En este sentido el sector Gobierno, el bancario y el de comunicaciones han estado a la vanguardia y pueden aleccionar a otras esferas.

Síntesis de aspectos que se deben tener en cuenta para la seguridad en compañías: Cuadro presentado por Jesús Jiménez.