Jahir Molina Zuleta
Los esfuerzos gubernamentales están dados pero hay sectores productivos que no están cubiertos por esa normatividad, donde no se identifica la necesidad de incluir riesgos informáticos a pesar de tener tecnología. Sería mejor esquematizar que la seguridad es para cualquier tipo de negocio y no solamente orientada a cumplir con una circular. De lo contrario va a quedar coja y seguiremos teniendo empresas donde es una moda y no una necesidad interna de ejecución.

Vicente Gozalbo
Desde el punto de vista de un fabricante de tecnología, Colombia es uno de los países que más ha crecido en proyectos de seguridad; lo que está en las circulares se está ejecutando y está enlazado con el tema financiero. La educación del usuario final es importantísima. Hay que enseñar a los hijos y a los padres para que sepan el riesgo de introducir información personal en las redes sociales.

Además, hace falta crear jurisprudencia, podemos tener las leyes pero si no denunciamos y si no empujamos los procesos judiciales para que se multe a las empresas tramposas y a los que cometen fraude, quedan sin aplicar.

Jesús Jiménez
En seguridad, el Gobierno está más avanzado que las empresas. Y entre las empresas privadas, las grandes son las que invierten porque las medianas y pequeñas no tienen el capital suficiente o lo ven como algo costoso.

Sandra Rueda, profesora
Hay un avance considerable pero hay partes en las que estamos rezagados, y es una de las razones de este foro: falta una visión integral del problema. Hay muchos elementos para tener en cuenta, como que en las juntas directivas haya personas que conozcan el tema, a todos los niveles estratégicos y de ahí hacia abajo, porque en el momento de tomar decisiones no solo se trata de certificarnos en ISO algo, sino lo que implica un proceso continuo.

¿Cómo ha luchado el Gobierno contra Anonymous? Si van a capacitar más gente en seguridad, ¿cómo garantizar que los *hackers*, sombreros negros o intrusos informáticos, no van a utilizar también la estrategia para sus fechorías?
Leonardo Huertas: Anonymous no se ha detenido; se le ha colocado un muro importante que ha reducido su actuar en el país. Eso ha sido gracias al trabajo coordinado del colCERT, del Centro Cibernético Policial y del sector privado.

Los delincuentes cibernéticos, los grupos activistas, están creando comunidades y preocupándose por prepararse; si nosotros no entramos en un proceso de capacitación continua con el Gobierno y el sector privado y si no trabajamos conjuntamente, no podemos garantizar que respondamos adecuadamente a estos delincuentes. Si están diseñando estrategias de ataque, con más razón debemos preocuparnos para defendernos.

¿Cómo venderle a un gerente, a un accionista, el proyecto que requiere la seguridad informática en la compañía?
Jahir Molina Zuleta: Ustedes saben cuánto pierden por tener una hora fuera de línea un sistema transaccional para sus clientes, o cuánto pierde su compañía, en imagen, en clientes, en credibilidad.

La alta dirección ve números. Váyanse a donde su financiero, y simplemente muestren que por tener una hora o 24 horas caída una plataforma se pierde tanto. Deben vender su tarea de seguridad como un negocio, es decir no genera gastos sino ingresos. ■

Se puede consultar la versión completa en
http://forosisis.uniandes.edu.co/seguridad-de-la-informacion/1er-foro-nacional-de-seguridad-en-ti/

Espiar o vender información personal es un delito

Vicente Gozalbo, de IBM Security Solutions, asegura que hay que comenzar por lo básico para que la gente entienda que fisgonear los correos o subir datos privados de terceros a las redes sociales puede llevarla a la cárcel.

Más allá de las recomendaciones obvias de seguridad, tales como no compartir la clave ¿qué se le puede enseñar al usuario final para que se proteja y la estrategia de la compañía sea fructífera?
Ahí está el quid del asunto. Cada vez encuentro más gente que desconoce que leer el correo electrónico ajeno da cárcel en prácticamente todos los países de la tierra. Desde pequeño te deben enseñar que la información es privada, personal e intransferible y debes respetarla. Subir a Facebook esa foto de un amigo en estado etílico es un delito porque atentas contra su privacidad y en la redes sociales hay muchos ámbitos en los que se están relajando los controles o haciendo que la

La gente desconoce que leer el correo electrónico ajeno da cárcel, dice Vicente Gozalbo, de IBM Security Solutions.

gente no se percate de lo malo que puede ser subir determinados datos a internet. Ya no se trata solo de las contraseñas. Hay otras cosas básicas que incluso las compañías desconocen como, por ejemplo, que los datos que reposan en sus sistemas no son suyos, sino de los clientes y ellas no pueden venderlos, traficarlos o cederlos sin su permiso. Eso está en todas las regulaciones. La legislación existe, pero falta jurisprudencia. En Europa, se aplica con mucho rigor pero aquí, basado en el contacto que tengo con militares y funcionarios del Gobierno, puedo decir que la ley no se aplica. Por eso hay que empezar a educar, porque si la gente sabe que eso no se hace, puede denunciarlo. Einstein decía que los errores más grandes vienen del desconocimiento de lo más básico. Hay que esforzarnos en dar visibilidad a esas cosas que ahora toman relevancia con tanta red social por internet.

¿Cómo convencer a las empresas de que la seguridad no es un mal necesario, sino una decisión estratégica, teniendo en cuenta que las inversiones son temporales porque de todas maneras sus sistemas serán vulnerables?

Como decía en mi charla es un balance, una decisión de compromiso. Debes estudiar muy bien tus vulnerabilidades y riesgos y cuánto dinero le quieres dedicar, pero también debes convencer a tu compañía con ejemplos reales de empresas que han conseguido negocios al invertir en seguridad. En nuestro congreso del año pasado, Whirpool relató cómo consiguió un retorno de un millón de dólares en su inversión cuando puso a disposición del público los manuales de los electrodomésticos en un servidor protegido y la gente debía pagar centavos de dólar por acceder a ellos.

> "La respuesta a por qué gastar dinero si de todas maneras voy a ser vulnerable a los ataques es muy fácil: porque no querrás que te suceda dos y tres veces. Si te tiene que suceder, que sea una vez y lo más tarde posible".

En cuánto a por qué gastar dinero si de todas maneras voy a ser vulnerable a los ataques, la respuesta es muy fácil: porque no querrás que te suceda dos y tres veces. Si te tiene que suceder, que sea una vez y lo más tarde posible.

¿Con qué periodicidad debe actualizarse la tecnología usada para seguridad?

Por la dinámica del sector, uno podría estar gastando dinero todos los días, pero las mejores prácticas establecen unos controles mínimos trimestrales para escanear los sistemas y detectar cuáles son vulnerables. También puede hacer revisiones anuales de la estrategia y establecer planes a cuatro años, pero lo importante es tener bien claro el objetivo e irlo revisando con periodicidad.