- Cuenta con una estrategia capaz de demostrar que la seguridad tiene retorno cuantitativo y cualitativo. "La banca es especialistas en decir invertí tanto y me ahorré tanto dinero, o mis clientes están contentos y transan más seguros".
- Cuenta con modelos de riesgo y cumplimiento maduros. ■

Germán Patiño
sales manager de
NoLA, Trusteer.

La banca móvil del futuro

Enfocado a la parte tecnológica, el experto Germán Patiño presentó cinco escenarios que ilustran hacia dónde va la banca móvil:

- **Pagos por ADN:** Se podrán transferir fondos con solo decirle a su celular: "Quiero pagarle a X, tanta cantidad de dinero".
- **Presupuestos personales inteligentes**. La banca se convertirá en asesora financiera en tiempo real, con aplicaciones de móviles, para suministrarle límites de sobregiro y patrones de previsión de gasto.
- **Banca sin fricción:** Con Tecnologías de Campo Cercano (NFC) al llegar al banco habrá un campo cercano de energía que transfiere una información a su dispositivo y tiene capacidad de intercambiar datos, saber su saldo o qué problema tiene.
- **Autopagos:** En cinco o diez años casi no habrá cajas de pagos y los clientes podrán pagar escaneando un código QC.
- **Dinero flexible y libre**: En la era del dinero plástico, cada vez este va a ser infinitamente trasferible y libre y más digital. "Ya hay gobiernos que se están enfrentando a problemas donde no manejan tasas de cambio con otras moneda, sino tasas de cambio con otro tipo de modelo económico".
- **Banca de realidad aumentada:** Con ella podrá poner una cita desde cualquier parte con su asesor financiero y a través de un aplicativo estar dentro del banco.

Las empresas pequeñas ven la seguridad como **un gasto**

En la sección de preguntas del público, los participantes en el Foro hablaron sobre logros y retos en seguridad.

En la primera parte respondieron a la siguiente pregunta:
¿Cómo ve el avance del Gobierno y de las empresas colombianas en la integración de políticas y mecanismos de seguridad a las estrategias de negocios?

Leonardo Huertas

Es importante definir el tema de integración de políticas en las compañías, porque todas las empresas y los sectores son diferentes. Se generan políticas y se ajustan de acuerdo con los requerimientos individuales.

Germán Patiño

En dos años tuvimos un avance importantísimo en seguridad como estrategia en el sector público y privado. Sin embargo, está rezagada la educación del usuario final. La fuerza de las inversiones se pierde si como clientes no tenemos una cultura.

De izquierda a derecha Guillermo Angarita, Jesús Jiménez, Vicente Gozalbo, Jahir Molina, Leonardo Huertas y Luis Edmundo Suárez.

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