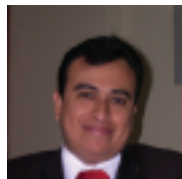
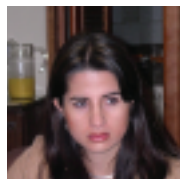
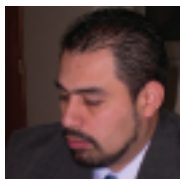
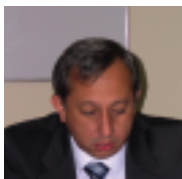


Inversión en Seguridad Informática, de la teoría a la práctica

Sara Gallardo M.

Representantes de Colpatria, IBM, Banco de la República, Deloitte y el DAS, invitados por la revista Sistemas, debatieron desde la orilla de sus propias vivencias.



Hace casi cinco años, la información ya era definida como el activo más valioso en cualquier espacio alrededor del mundo. Después de los ataques a las torres gemelas de New York, el 11 de septiembre de 2001, además de mantenerse en esa cima se convirtió en uno de los más vulnerables y, como si fuera poco, en el punto de partida de cualquier tipo de ataque o el motor de distintos actos delictivos.

Desde entonces, la seguridad camina de la mano con la información, de otra manera. En algunos ambien-

tes, cumpliendo con todos los requisitos y en otros, siendo apenas objeto de aproximaciones.

Para analizar el panorama colombiano de cara a esos temas, Jaime Eduardo Santos, vicepresidente secretario de Banca Colpatria; Juan Carlos Huertas, director de la Unidad de Seguridad Informática del Banco de la República; Wilmar Castellanos, gerente de Riesgos y Servicios Corporativos de Deloitte; Ana Verónica Carreño, especialista en Seguridad de IBM; y, Carlos Baquero, analista de Sistemas del Departamento Administrativo de Seguridad

(DAS), participaron en el tradicional foro de la revista Sistemas.

Los invitados fueron recibidos por Jeimy José Cano, presidente de la Junta directiva de la Asociación Colombiana de Ingenieros de Sistemas (ACIS); Francisco Rueda, director de la revista; Julio López, miembro del Consejo de Redacción de la publicación y moderador del foro; Beatriz Caicedo, directora ejecutiva de ACIS; y, Sara Gallardo, editora de la publicación, organizadora del debate.

Julio López M.

¿Cómo está organizada el área de seguridad en su empresa?

¿Seguridad y seguridad informática están integradas? ¿Tienen presupuestos diferentes?



Julio López M., moderador del foro

Jaime Eduardo Santos Mera
Vicepresidente Secretario
Multibanca Colpatría



El área de seguridad en Multibanca Colpatría depende del Vicepresidente Secretario, funcionario con formación jurídica con 20 años de experiencia profesional como abogado corporativo. La Vicepresidencia tiene dos líneas de reporte, a saber: una a la Presidencia de la Junta Directiva y otra a la Presidencia del Banco. La primera línea de reporte con alcance al grupo empresarial Colpatría como seguridad y la segunda de naturaleza jurídica, con un reporte exclusivamente a Multibanca Colpatría. Eso implica que el modelo de organización de la seguridad en la entidad forma parte de la toma cotidiana de decisiones de gobierno.

A su vez, la Vicepresidencia cuenta con varias dependencias . La jurídica

que contempla litigios y aspectos legales preventivos; la secretaría general, que cumple el apoyo de los órganos societarios y de los accionistas; un área de control de lavado de activos; y, la de seguridad entendida como la responsable de toda la investigación de fraudes corporativos y de la protección física de las personas y las instalaciones.

Esa forma de organización corporativa nos permite tener todo el tiempo unos vasos comunicantes entre expertos de distintas disciplinas que cooperan entre sí, de forma permanente. Así, por ejemplo, ante una queja por un fraude en un cajero electrónico, que llega al área legal, para conceptuar sobre la responsabilidad del banco, se tiene el apoyo inmediato del área de seguridad, para establecer los hechos con precisión técnica. Es decir, se logra un ejercicio de sinergias entre expertos en el que el rol del Vicepresidente es el de moderador de disciplinas, evaluador y medidor del riesgo para la organización.

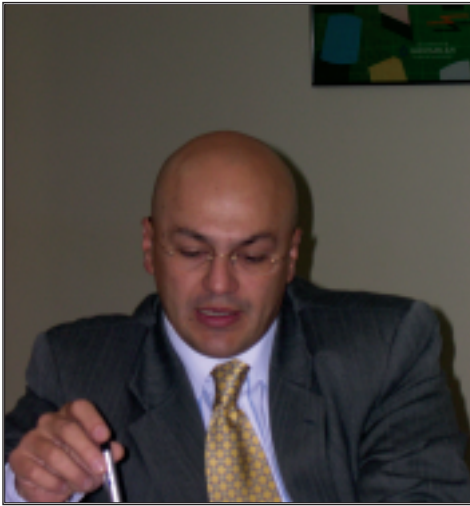
El área de seguridad es interdisciplinaria, compuesta por un grupo de ingenieros de sistemas, sociólogos, abogados, contadores, administradores bancarios y criminalistas. En este momento estamos en el proceso de selección de un antropólogo, pues consideramos que esta disciplina aportará otra visión para el análisis de la criminalidad.

Así mismo, tenemos la gerencia de seguridad informática, que tiene a cargo la protección de los bienes informáticos y el control de quienes sobre ellos actúan, desde adentro o fuera de la organización. Depende de la Vicepresidencia de Operaciones y Tecnología y tiene un reporte funcional con el Vicepresidente Secretario, para coordinar las actuaciones y establecer hipótesis conjuntas de trabajo.

En resumen, podemos afirmar, para cerrar la pregunta, que el área de seguridad de Colpatria hace parte de la estrategia en el modelo de gobierno y por lo tanto se ubica en la alta dirección y cuenta con un equipo de trabajo profesional e interdisciplinario.

Juan Carlos Huertas
Director Unidad Seguridad
Informática
Banco de La República

El área de seguridad informática en Banrepública tiene alrededor de 18 años de creada, trabaja independiente y está en un nivel tres de la organización (Dirección). Dentro del organigrama figuran en su orden el nivel de Gerencia (Gerente General, Gerencia Técnica y Gerencia Ejecutiva), el nivel de subgerencias, dentro del cual se encuentra la Subgerencia de Informática; y el nivel de direcciones. Para el caso de la Subgerencia de Informática se tienen cuatro direcciones: la primera se



Juan Carlos Huertas

encarga de los desarrollos corporativos y en general de la ofimática (gestión de micros y su correspondiente software) del Banco; la segunda es responsable por toda la plataforma de redes, servidores (hardware-software) y centros de cómputo; la tercera es responsable del centro de soporte informático y las estrategias de continuidad informáticas del negocio. Finalmente, la cuarta área es la Unidad de Seguridad Informática encargada de todo lo referente a la seguridad de la información.

En esta última área trabajan alrededor de 14 ingenieros en función netamente de seguridad informática, no de seguridad física. Trabajamos muy alineados con el pensamiento estratégico del Banco. Hace poco logramos la certificación ISO 9001 en temas de procesos. También trabajamos acorde con las recomenda-

ciones de las áreas de control del Banco, y disponemos además de unos espacios por demanda en algunos comités de alto nivel, presididos por el gerente ejecutivo.

Trabajamos también en función de políticas, estándares y mejores prácticas sobre temas tales como el desarrollo de tecnologías sobre el tema, riesgos y administración de seguridad informática.

Verónica Carreño
Especialista en Seguridad
IBM



En IBM los requerimientos de seguridad varían porque se trata de una compañía proveedora. Tenemos dos áreas. La primera tiene que ver con operaciones y control de procesos. La segunda está encargada de la infraestructura y aseguramiento del riesgo. Las dos se interrelacionan para tratar asuntos con la responsa-

bilidad que le damos al usuario. De cara a los usuarios estamos en el proceso de culturización para obtener mejores prácticas; para ello, los relacionamos con nuestras herramientas de seguridad como IAS, a través de la cual el usuario es consciente del cumplimiento de ciertos lineamientos establecidos con anterioridad.

El usuario es entonces consciente de que tienen que cumplir con ciertas políticas de seguridad para poder ingresar tanto a las redes, como a diferentes contenidos dentro del medio. Son dos directrices diferentes. Una reporta a operaciones y otra directamente al área de informática.

Wilmar Castellanos
Gerente de Consultoría de Riesgos
Deloitte



Deloitte, es una organización Global. Para gestionar la Seguridad de la Información, existe el Global Infor-

mation Security Office, que tiene diferentes funciones relacionadas con la definición de políticas y estándares de seguridad de la información y de la seguridad física, no solo de la información y de los equipos de cómputo sino también de la gente, por ejemplo, cuando se requiere el desplazamiento de nuestros profesionales a otros países o a zonas consideradas riesgosas.

Esta misma oficina administra los temas de continuidad de operaciones y coordina todo el plan de contingencia y de recuperación ante desastres, los esquemas de protección antivirus, y en general, estándares de seguridad de la firma.

Existen dentro de la organización políticas claras y perentorias sobre el uso de los recursos de información como el correo electrónico, por ejemplo. En la empresa la información, especialmente la relacionada con los clientes es de alta relevancia.

Julio López M.
¿Cree usted que su organización invierte en seguridad informática lo necesario para su protección (desde un punto de vista práctico), se excede o es deficiente? Ilustre su respuesta.

Jaime Eduardo Santos Mera

Yo vería esta pregunta desde los resultados económicos para la orga-

nización. Multibanca ha logrado, en los últimos años, reducciones en las primas de seguros de póliza global bancaria y de fraudes con tarjetas de crédito, incluso en esta última de devolución en primas. Para mí, se trata de un indicador económico que ilustra cómo se ha hecho una inversión en seguridad adecuada para proteger a Multibanca y a sus clientes. Para citar un ejemplo, un consultor con prácticas internacionales, nos acaba de hacer una evaluación de la seguridad informática, en la cual refiriéndose a porcentajes, nos dice que nos ubicamos en niveles de cumplimiento del 80%, frente a referentes internacionales y en indicadores del doble en relación con referentes en Colombia. Eso me permite decir que tenemos un trabajo consciente y una inversión en recursos suficiente, en el entendido que siempre todos queremos mejorar lo que tenemos, pero sin perder la relación costo -beneficio.

De otro lado, el cambio del proceso penal en Colombia hacia un sistema acusatorio nos ha llevado a incurrir en unos gastos adicionales, como por ejemplo en el mejoramiento de la cadena de custodia y el uso de software mas amigable para el procesamiento de las investigaciones, de tal manera que sea fácil explicar a las autoridades los hechos por nuestros peritos expertos. Ahora las investigaciones se desarrollan dentro de un flujo grama debidamente documen-

tado, que demanda tiempo del recurso humano, en su nueva condición de peritos expertos.

De cara a este panorama, se requiere de personas con perfiles distintos, por ejemplo, ingenieros de sistemas con una visión más amplia para poder desenvolverse cuando tengan que sustentar ante un juez, en una audiencia pública, los aspectos de una determinada situación.

Por tales razones, el tema probatorio es muy importante mirarlo con relación a los costos.

Juan Carlos Huertas

En el Banco la seguridad es un tema prioritario y en términos de recursos han sido suficientes. En lo que sí puede haber alguna oportunidad de mejorar -como sucede en la mayoría de organizaciones-, es en el tema de recurso humano para atender todos los asuntos del área. Existen temas adicionales que quisiéramos abordar (velar por el cumplimiento de las políticas dentro de la organización, los aspectos jurídicos con la dimensión de tiempo, vigilar lo que sucede con los documentos que antes se manejaban en papel y ahora en forma electrónica, la atención de incidentes, el hacking y el hacking inverso). Se trata de hacer inteligencia de hacking para contemplar situaciones hipotéticas e ir mucho más allá de la herramienta para detección de intrusos.

Por otro lado y no menos importante, queremos dedicar tiempo e investigación en torno a la informática forense para estar preparados y contar con un grupo élite en función de escenarios probatorios de evidencia electrónica, en ambientes jurídicos. Pretendemos alinearnos a las mejores prácticas, en particular con el BS 7799. Todo ello, en función de habilitar nuevas oportunidades tecnológicas para el negocio.

Es necesario introducirnos en la investigación y, por supuesto, trabajar en los riesgos para la organización, desde un enfoque global y del sector financiero, acciones que deben proyectarse más allá de las puertas físicas de la entidad.

Ese panorama se orienta al hallazgo de un gobierno de la seguridad de la información dentro del Banco y, en esa medida, replantea un nuevo reto en para la organización.

Verónica Carreño

El enfoque que tiene IBM es el de proveedor de servicios y en ese sentido, tiene diferentes portafolios. Dispone de lo que se llama BCS Business Consulting Services, es decir, un equipo de seguridad enfocado a diferentes tipos de empresas, entre las que se cuentan las más grandes que aparecen publicadas en la revista Fortune 500, hasta las medianas y pequeñas, hacia donde

empezamos a dirigir también esfuerzos.

Bajo esa infraestructura se observan las amenazas de seguridad, se realiza inteligencia para determinarlas en términos de estadísticas y reportes de cada una de las organizaciones.

De cara al software, tenemos un portafolio de seguridad enfocado a las diferentes capas. La primera tiene que ver con la seguridad perimetral en la que hablamos de las amenazas, del estudio forense, de las amenazas relacionadas con detección de intrusos, correlación de amenazas reportadas en los diversos dispositivos de seguridad y ejecución de ciertas tareas que ayudan a bloquear en tiempo real ataques a ciertos recursos.

En otra capa más profunda abordamos la gestión de identidad, porque las amenazas están cambiando. Nos hemos dado cuenta de que a medida que aumenta la fortaleza de las redes y la seguridad en ellas, aparecen empresas dedicadas a hacer fraudes mediante el robo de identidades. Algunas cifras en Estados Unidos señalan que alrededor de nueve mil personas promedio, son suplantadas mensualmente, como consecuencia de las acciones alrededor de la ingeniería social. Tales delincuentes establecen relaciones de confianza para obtener la información y eso se da dentro de las organizaciones. Para atacar este tipo de amenazas se han

construido soluciones que permiten un control más activo de la creación y acceso de usuarios a los diversos recursos empresariales basados en políticas y en roles organizacionales que se ven mapeados dentro de la solución.

Una tercera capa corresponde al resumen sobre el cumplimiento de las políticas. Es necesario observar que las políticas establecidas en la estratosfera se ejecuten en la práctica. Esta capa es la encargada de posicionar, revisar y diagnosticar el cumplimiento de políticas de seguridad que se han definido previamente basadas en estándares y requerimientos particulares para cada empresa.

Así mismo, tenemos unos expertos en seguridad que producen reportes mensuales y periódicos de los diferentes campos de las amenazas, dichos reportes vienen de un estudio exhaustivo de las amenazas más comunes en los clientes que vienen siendo monitoreados por los servicios de IBM y que han reportado grandes amenazas que pueden repercutir en las diversas industrias.

Wilmar Castellanos

Dadas las características de nuestra organización, tenemos que estar muy al tanto de la tecnología y sus aplicaciones. Somos pioneros en la inversión en seguridad, ya que esto es

parte de mantener la confianza de nuestros clientes. En la auditoría, que es el negocio más grande de la firma, es imprescindible contar con mecanismos de protección adecuados para la información. No solo a nivel de controles técnicos, sino de la seguridad de las personas.

Para cumplir y mantener una adecuada seguridad y protección de la información por parte de nuestros profesionales, las personas de la firma deben cumplir con un número importante de horas de entrenamiento relacionado no sólo con estándares de auditoría, sino con estándares profesionales relacionados con ética, independencia, confidencialidad y manejo de relaciones con los clientes. Este es uno de los rubros de mayor inversión por parte de la firma.

Las políticas de la firma en cuanto a inversión de seguridad son muy conservadoras, teniendo en cuenta que debemos implementar continuamente una cantidad importante de controles para proteger la información.

Sara Gallardo M.

De acuerdo con lo expuesto por Jaime Eduardo Santos de Colpatria, ¿cómo se enmarca la labor de un antropólogo dentro del tema de seguridad informática? Despierta curiosidad esa nueva propuesta.

Jaime Eduardo Santos

Se trata de aplicar la teoría 'del cabello verde' junto al "cabello blanco" que consiste en que en los equipos de trabajo de alto desempeño deben participar personas sin ningún paradigma y personas con experiencia, para de su combinación alcanzar hipótesis de trabajo innovadoras y aplicables a la realidad específica. Es así como decidimos contratar una persona que tuviera alrededor de 23 años, que hablara más de dos idiomas, que fuera egresado de una universidad de primer nivel y que no supiera nada de seguridad ni de banca, que llegara libre de sesgos ocupacionales. Una persona de unas características muy distintas, comparada con el resto de la organización. Después de estudiar la teoría se encontró que los antropólogos tienen dos fortalezas. La primera, un rigor científico profundo, son expertos en método. Y lo segundo, que un psicólogo llamaría una alta tolerancia a la frustración. Ellos -los antropólogos-, pueden trabajar durante 30 años buscando una 'monedita', no encontrarla y no morirse por esa razón. Caso contrario al de los abogados, que son poco tolerantes en caso de perder los pleitos.

Francisco Rueda

Con base en la experiencia de los proveedores, ¿cuál es en promedio, la inversión de las empresas colombianas en

seguridad? ¿se puede mencionar o es confidencial?



Francisco Rueda

Wilmar Castellanos

Los proveedores de la tecnología han cambiado el mercado de tecnologías de seguridad. Antes los firewalls u otros dispositivos de seguridad eran un elemento diferenciador, así como tener presencia en Internet. Hoy en día son una necesidad para cualquier organización. Actualmente las empresas piensan en sus necesidades de seguridad a largo plazo, no sólo en soluciones tecnológicas puntuales de seguridad, por esa razón el alineamiento de la estrategia de seguridad de la organización con estándares como ISO 27001 es imprescindible. En este mismo sentido, las organizaciones comenzaron a explorar una serie de herramientas y referentes para llevar

la seguridad a un enfoque por procesos y basado en análisis de riesgos para la información, permitiendo establecer una estrategia de seguridad que soporte las decisiones de inversión en seguridad.

Existe mayor conciencia de que invertir en seguridad no es comprar lo más nuevo en tecnología, sino que debe obedecer a un proceso detallado de análisis de riesgo con base en la información que se maneja en los procesos de negocio. La información implica criticidad para el negocio en términos de imagen, clientes y valor para los accionistas.

Por eso las inversiones son más consecuentes con los requerimientos de la organización, más que con la adquisición de herramientas específicas de proveedores específicos.

Carlos Baquero
Analista de Sistemas
DAS



Nosotros tenemos un entorno bien diferente al de la empresa privada, porque se trata de un activo muy importante. Lo que hemos hecho más allá del software y hardware - porque la seguridad informática es más que eso-, ha sido cuidar mucho la cultura de la información. Sobre la pregunta que nos compete, también hemos invertido una buena suma de dinero en seguridad informática a nivel de tecnología (hardware y software). De hecho, lo que nos pasó hace poco, bien conocido por todos, no tuvo nada que ver con la tecnología misma, sino con las personas desde adentro de la organización. Eso nos ha permitido capitalizar la experiencia y trabajar mucho con el recurso humano, porque tenemos unos muy buenos sistemas de seguridad, pero lo que no pensábamos o con lo que no contábamos era que nos iban a vulnerar desde adentro. Eso nos dejó ver que la inversión debía enfatizarse en la cultura informática a nivel de nuestra organización. A partir de ese incidente creamos un cuerpo de especialistas que se va a encargar de las bases de datos, de recursos. Uno debe tomar de las experiencias lo más importante, y aunque fue un episodio bien difícil, nos permitió identificar ese tipo de debilidades que inclusive en las empresas privadas poco se tiene en cuenta. Todos queremos máquinas robustas, buenos firewalls, buenos sistemas que nos detecten vulnerabilidades, pero el ambiente

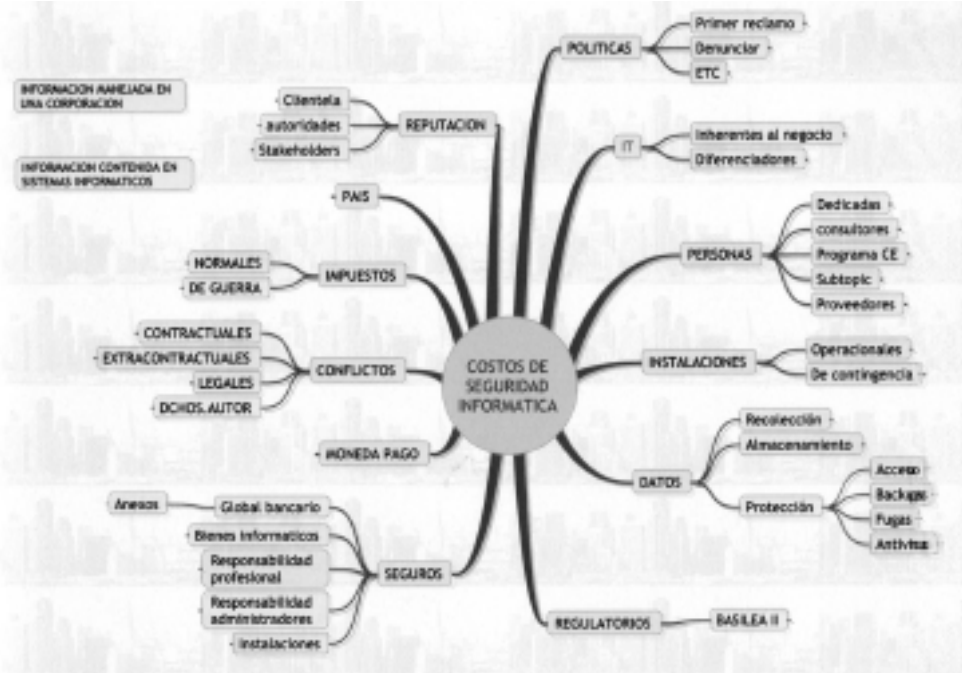
interno desde el recurso humano se descuida. Con la ayuda del Gobierno Nacional estamos haciendo inversiones en esos temas relacionados con la seguridad de la información desde adentro de la organización.

Julio López
¿Cuáles son los principales

rubros de costos asociados a la seguridad de la información en su organización?

Jaime Eduardo Santos

Es complejo discriminar los rubros de gastos por lo cual elaboré un mapa mental para tratar de organizar mis palabras.



El mapa no está escrito dando prioridades, sino dejando ver un panorama para comentar con ustedes dos o tres rubros. El primer costo en seguridad yo lo llamo el de las políticas. Tener o no tener políticas es ya un costo. Multibanca por ejemplo tiene como política el pago de primer reclamo de un cliente cuando se ubique en un determinado perfil de riesgo. El

banco le cree y pueda que me esté tumbando, pero por política estoy ya asumiendo un costo. El costo de denunciar. Como ciudadanos tenemos la obligación de denunciar, pero al concretar la denuncia ante las autoridades se presentan dificultades que implican poseer principios de colaboración bien cimentados que permitan una visión integral de lo



Uno de los rubros asociados a la seguridad corresponde a la tecnología de la información, anotaron los participantes.

privado con lo público. Esto implica la asignación de recursos, por ejemplo en peritos, para hacer en forma adecuada una acción de protección a la empresa que uno representa y a la sociedad por la obligación que tiene de denunciar. Otro rubro de costos asociados a la seguridad, es el de la tecnología de la información, y este lo divido en, los costos inherentes al negocio, cosas que el banco debo mantener para funcionar cada mañana. Estos costos son los mas difíciles de identificar, porque la tecnología ya viene con muchas seguridades incorporadas. Los otros costos que sí hacen una diferencia son los que yo llamo diferenciadores, los que me dan beneficios frente a los competidores. Así por ejemplo si el banco se quiere diferencia en el segmento de tarjetas de crédito, hace una inver-

sión especial en un software para colocar unos determinados filtros y poder proteger más sus clientes. Entonces hay costos que no le dan un valor agregado a la organización, son necesarios para prender la maquinaria, poner en marcha la fábrica. Otros costos importantes son los de personal, que igualmente los divido entre personas que están dedicados al tema exclusivamente y los que no. Entonces los primeros normalmente son la parte menor, frente al resto, toda vez que son temas culturales, se debe involucrar a toda la gente con la seguridad. En este punto en Multibanca tenemos como característica del trabajo permanente con la gente, que es algo que consideramos que nos hace un elemento de diferenciación y que nos ha permitido redimensionar cosas importantes

como las primas de seguros. La atención principal es hacia la gente, no hacia la tecnología, pues somos los humanos los que la usamos o abusamos de ella. Y dentro de esta atención buscamos un buen ambiente laboral en concurrencia con un programa de conocimiento del empleado desde su selección y durante su permanencia en la organización. En este programa nos hemos apoyado en expertos en comportamiento humano y en la combinación de herramientas de perfilación como de juicios de valor, estas son ciencias imprecisas y con información incompleta, pero se va progresando en conclusiones. El otro rubro que trabajamos es la seguridad de instalaciones. Y las agrupé en dos en el mapa conceptual. Las operacionales, las de todos los días que se requieren para poder estar en este negocio y las de contingencia, que deben estar disponibles ante un siniestro. Este rubro es el que más le cuesta al Banco, de cara al plan de continuidad del negocio. El plan de continuidad informática, como parte del plan de continuidad del negocio esta construido pensando en los programas de misión de crítica. Todo el plan de continuidad tecnológica esta contratado con un tercero experto y funcionando en otro lugar de la ciudad. Otro rubro de los costos tiene que ver con todo lo relacionado con los datos, desde la recolección hasta la protección. Todo lo de antivirus y

representa también costos. Siguiendo el mapa están los costos regulatorios que nacen desde Basilea y aterrizan en regulación nacional. El primer costo y el más grande de todos es empezar a construir las bases de datos a las cuales se les aplicaran modelos estadísticos predictivos. A manera de ejemplo, tenemos lo ocurrido con el sistema de administración de riesgos de crédito, que dejo como enseñanza que hay que tener los datos completos porque la tecnología para estudiarlos está ahí. Los seguros son otro rubro bastante importante al igual que el valor del dólar, toda vez que son servicios referenciados a moneda dura, luego en los costos de seguridad se deben tomar decisiones de inversión y gasto financieramente bien construidas para poder ser eficientes en los requerimientos de seguridad en los presupuestos de nuestras organizaciones. El otro costo son los conflictos legales y contractuales, el más obvio se refiere a los derechos de autor y el alcance de las licencias sobre el software. Entonces todo riesgo contractual tiene unos costos, porque muchas veces se gana, otras se pierde y otras se arregla. Otro costo en seguridad informática es la parte tributaria pues los bienes informáticos para seguridad se gravan cómo si se tratara de otra mercancía, pero en la banca estamos protegiendo de alguna manera al país de la criminalidad que atenta contra el

servicio público bancario. Los otros rubros del costo los llamo país, estar parado en Colombia cuesta distinto. El ejemplo más claro son los cajeros automáticos. Por estar parado aquí tenemos que inventar unos anclajes distintos a los que tienen que tener en otras partes. También los petardos, el fleteo, y demás son costos por estar ubicados en el país. Y el último y que no es cuantificable es la reputación. ¿Puede una institución financiera llegar a desaparecer por un solo incidente? Es la respuesta que ninguno quisiera conocer en su patrimonio por lo cual es el factor más importante a cuidar y para cuidarlo hay que tener funcionando en perfectas condiciones todos los factores comentados en esta reunión.

Juan Carlos Huertas

En el Banco manejamos rubros asociados a la inversión, hardware, software. Rubros asociados a los gastos en seguridad de la información y en general a la tecnología de la información. Dentro de la inversión los rubros más importantes asociados con seguridad son los servicios de monitoreo 7 x 24, como los puntos críticos de la plataforma en contra de un ataque o algo parecido. Así mismo, las tecnologías de control de acceso al Banco son un rubro relevante dentro del presupuesto. Sobre autenticación el Banco ha invertido y ha trabajado bastante. Por ejemplo, en autenticación con tecnologías de

firewalls y esquemas de autenticación basados en dos factores. Hoy en día estamos en vías de ejecutar un presupuesto importante en una arquitectura denominada seguridad orientada a servicios, en el nuevo enfoque que le queremos dar a la seguridad en el Banco. En otro sentido, antes nos preocupábamos mucho por los agentes externos, ahora lo hacemos por la situación de adentro.

Todo el tema de gestión de vulnerabilidades, firewalls internos, detección de intrusos son rubros importantes dentro de ese presupuesto de hardware y software. El rubro de gasto es enorme porque como bien lo mencionaba Jaime el tema es mantener la seguridad. Otro rubro importante es el recurso humano que trabaja en seguridad, esos costos de mantener esos profesionales de planta es también una inversión que hace el Banco en función de la seguridad. El tema de continuidad del negocio es un tema también muy importante. Nosotros ya vamos para un tercer centro alterno ubicado por fuera de Bogotá. Tenemos un centro alterno También dentro de la póliza global bancaria hay unos costos asociados dentro del tema de seguridad y yo diría que esos son los rubros más importantes.

Francisco Rueda

¿Es posible determinar esos rubros en porcentajes, desde

aspectos tales como las personas y la tecnología?

Juan Carlos Huertas

Lo que podría decir en general es que el Banco puede estar oscilando entre un 3 y un 5% del presupuesto asignado a tecnología de información al tema de seguridad. Y es una cifra muy importante no incluyendo los costos relacionados con la continuidad tecnológica.... No necesariamente obedece a un tema específico de seguridad, obedece al tema de disponibilidad de servicio. Ahí podemos estar mezclando cosas que no son estrictamente de seguridad. Todos giran en función de la continuidad del negocio, pero no necesariamente desde la óptica que un atacante vaya a tumbar un servicio y eso sería un rubro asociado a seguridad. Entonces ese lindero se vuelve a veces complicado de demarcar. Pero, en general, uno podría decir que el Banco maneja algo de ese estilo.

Jaime Eduardo Santos

En el caso del banco la seguridad informática es del orden del 5% del presupuesto de tecnología, sin tener en cuenta el plan de continuidad tecnológica.

Julio López

A los representantes de IBM y Deloitte, les pido enfocar la

respuesta más desde el punto de vista de los clientes. ¿Cuáles son los principales rubros que ellos consideran en el entorno que estamos tratando?

Verónica Carreño

En realidad no es muy distinto a lo que ya hemos mencionado. En el ambiente empresarial se está observando una migración de los costos de seguridad, no lo que se refiere a Firewall o antivirus, sino la parte del control de la identidad, en la parte donde las empresas están tratando de potencializar usuarios y están haciendo que sus sistemas sean más robustos en todo lo relacionado con suplantación de identidad, también con el objeto de establecer un estándar común para todos los recursos, una manera de poder compartir servicios entre organizaciones.

Requerimientos comunes que expresan las compañías en la actualidad son; búsqueda de la manera en donde estén seguros y puedan ser auditables con información válida y coherente, cumplimiento de políticas relacionadas con auditoría.

Otro tema también importante cuando consideran incursionar en una solución de gestión de identidad es la disminución del costo operacional, en la medida en que muchas organizaciones los usuarios internos, los proveedores y clientes que entran

y salen son muy difíciles de controlar, entonces están buscando herramientas que les ayuden a no tener una persona dedicada a ese tema sino que sea un tercero. No que sea una gestión día a día.

En lo que se refiere de recuperación de desastres, es un tema también muy importante, ellos tienen que saber cuáles son los sistemas críticos, cuáles de dichos sistemas son los que requieren alta disponibilidad y cómo se va a seguir un plan de recuperación ante desastres. Por ejemplo, en el caso de una catástrofe general, tanto el sistema como los datos que se hayan perdido deben tener mecanismos que los puedan respaldar. Esos son los dos fuertes que vemos en la actualidad.

Wilmar Castellanos

Hablando un poco sobre el mercado, ¿qué tendencias se observan?. En esta mesa las personas son representantes de organizaciones que desde el punto de vista de negocios son pioneras en temas de seguridad, debido al negocio en el que están, p. e. bancos, seguridad estatal, banco central. En el tema de inversión en seguridad de la información, este tipo de organizaciones que ya han recorrido un camino importante en el tema de seguridad, están hablando de inversión en seguridad de la gente y de la seguridad de la tecnología de información. Hoy día es importante

saber quién es la persona que estoy contratando y quién es la persona con quien trabajo. No solo en el momento de la contratación, sino durante su permanencia en la organización. En la medida en que una persona crece dentro de una empresa, tiene acceso a información cada vez más sensible, y sus acciones, buenas o malas, tienen un mayor impacto dentro de la organización.

En este sentido uno ve que las organizaciones más avanzadas en seguridad de la información claramente han enfocado esfuerzos y presupuesto en temas de seguridad de la información basada en personas, focalizando temas como conciencia de seguridad, sensibilización de la gente, que la gente esté convencida de que el tema de seguridad no es impuesto por la organización y responsabilidad sólo de unos pocos, sino que compete a todos los miembros de la organización. También es claro que las organizaciones están invirtiendo mucho más que antes en servicios y en consultoría de seguridad, y con un foco diferente, porque los firewalls u otras tecnologías, a pesar de ser una necesidad, en muchas ocasiones no dan valor agregado.

La tendencia de muchas organizaciones a comprar tecnologías de seguridad, simplemente por la buena labor comercial de los proveedores más que por un valor para el negocio,



Desde la óptica de los proveedores, para gestionar la seguridad es importante contar con servicios profesionales adecuados, y para ello es necesario invertir.

hizo que muchos de los servicios profesionales fueran entregados de manera gratuita por proveedores de software o hardware, ya que su objetivo principal era vender tecnología. Hoy en día las organizaciones empiezan a ser conscientes de que el servicio que deben contratar debe ir más allá de la instalación de un equipo o de la misma evaluación puntual de vulnerabilidades. Aquellas organizaciones que no tienen internamente ciertos recursos especializados en seguridad, han identificado la necesidad de contar con un tercero que pueda suplir ese conocimiento para cumplir con funciones específicas de seguridad, y más importante aún, para ayudar con actividades como:

- El alineamiento de la seguridad en la organización con normas internacionales

- La definición y la asignación de roles.
- Sensibilización de personal en aspectos de seguridad.
- Obtención de información sobre la percepción de la gente de la organización sobre los temas relacionados con seguridad.

Claramente la tecnología sigue siendo más costosa que los servicios profesionales, pero también es claro que el impacto de no invertir en la gente o en servicios profesionales adecuados para gestionar la seguridad puede revertirse después en un costo muy superior al de la tecnología misma.

Jaime Eduardo Santos

Al observar la clientela del banco en situaciones de fraude encontramos

en muchos casos que no están involucrados en la problemática y requieren consultoría al respecto. El cliente se acerca a la institución diciendo me robaron. Entonces le pedimos revisar lo que pasó y resulta que nunca ha tenido el concepto de seguridad en la cabeza y por lo tanto ha sido afectado en algunas ocasiones por sus propios empleados y en otras por empresas criminales que transitan por el mundo financiero buscando oportunidades para atacar. En estos clientes no solo encontramos personas naturales sino empresas importantes en el país.

Wilmar Castellanos

Más allá del sector financiero, en las organizaciones del sector real uno ve que las prioridades de inversión tienen que ver más con volver más eficiente su producción, con mejorar la producción y sus costos asociados, y con el control de calidad del producto. El perfil de la gente en estas organizaciones hace difícil incorporar la seguridad de la información de manera consistente, ya que sus prioridades apuntan a la productividad, lo cual puede reñir con temas como el cambio periódico de contraseñas o con cierre de sesión en los sistemas después de 30 minutos de inactividad. Igualmente, la gestión de la seguridad de la información no genera un impacto social tan alto como el que genera en organizaciones del sector financiero.

Carlos Baquero

Para responder a la pregunta me voy a referir a tres aspectos muy importantes que nosotros hemos tenido en cuenta. Como sector público concientizar a planeación y a presupuesto de que nos de dineros para invertir en seguridad que es un activo prácticamente intangible, nos ha costado muchísimo trabajo. Aún así yo hablaría sin especular que hemos dedicado una suma importante para todo lo que tiene que ver con seguridad, porque debe ser nuestro fuerte. Yo hablaría de un 3 o 4% en un rubro general que el Estado designa para temas informáticos y de tecnología. Pero nos ha costado mucho llegar a eso. Realmente nos preocupábamos más por otras cosas. En nuestro caso por armas, chalecos blindados y cosas de ese tipo que son importantes pero sobre concientizar a la persona, el estudio tampoco lo hacen porque no hay una verdadera conciencia de que lo que se va a invertir va a perecer. Y si hablamos de invertir en talento humano, el personal que se dedique netamente a seguridad informática es mucho más débil, porque es la persona máster en seguridad, pero si él llega a morir, los conocimientos de él no son transmitidos a las demás personas del grupo. Se trata de un tema muy cerrado.

Julio López

Las medidas de contingencia en seguridad informática, nor-

malmente son redundantes y representan una inversión alta para toda organización. En su caso, ¿qué porcentaje de estas medidas (o de los costos asociados) es utilizado para mejorar los servicios prestados (uso compartido) y cuál es el restante?

Jaime Eduardo Santos



En la pregunta tres contesté lo que tenía que ver con la cuatro. Tal vez adicionar que nosotros contamos con una continuidad del negocio permanente. Es un ingeniero de sistemas de dedicación exclusiva y esa persona es quien coordina toda la organización. Desde un equipo que llamamos EL ERI, equipo de reacción de incidentes, pasando por el COE que es el comité operativo de emergencias y llegando al plan de continuidad de negocios. Esa persona relaciona los tres temas y eso

moviliza a toda la organización. También cito un ejemplo, si en este momento estamos en campaña electoral entonces ponemos nuestras instalaciones en una x alerta, se activan todos estos comités y esta persona está pendiente de que todas las cosas estén coordinadas y que todas las cosas que se han llevado a prueba durante todo el año, en este mes las tiene que expresar para ver que estemos listos para cualquier eventualidad. Hay un trabajo permanente y necesariamente coordinado para todas las áreas de la organización.

Juan Carlos Huertas



En este momento estamos en una estrategia de acercarnos mucho al tema de mejores prácticas en seguridad de la información en el proceso de contratación. Trabajamos con Recursos Humanos para oficializar en un corto plazo incluir una cláusula específica de términos, políticas

de seguridad informática y generar directrices de seguridad de la información. También se incluyó un capítulo dentro del proceso de inducción a los empleados que tiene que ver con seguridad de la información. En general, lo que tiene que ver con continuidad del negocio, y particularmente continuidad con seguridad de la información participan todas las áreas del Banco. La entidad está en un proceso de autocontrol en donde se está descentralizando de alguna manera esa función. Es decir, la continuidad del negocio y la gestión de riesgos no deben ser algo exclusivo del área de seguridad o del área de tecnología. Lo que estamos haciendo nosotros es cada vez más, gracias al apoyo de la alta gerencia, transmitir la idea de que la seguridad es una función implícita dentro de cada una de las áreas de negocio del Banco. Y eso ha sido muy importante, porque muchas áreas ya han despegado en eso y hacen sus propios ejercicios y pensamientos de continuidad en función del riesgo, en función de tecnología y de operación de manera autónoma, ya no dependiendo tanto de las áreas técnicas. Eso es un punto importante. Por otro lado, cuando hablamos de la importancia de las estrategias de seguridad en función de la continuidad del negocio yo lo vería de la siguiente forma. En general, una política del Banco es que cualquier tecnología o cualquier plataforma que sea base para el funcionamiento de negocios corporati-

vos sensibles, debe estar multiplicado por dos. Es decir, no debe haber cuellos de botella en ningún sentido. Y vamos hacia una, en algunos servicios, a que eso sea por tres. En términos de estrategias específicas de seguridad en continuidad diría que es de la mayor importancia, en el sentido de que hay partes o componentes de seguridad que si dejan de funcionar el negocio deja de funcionar. Y me refiero, por ejemplo, al portal de acceso a los servicios corporativos. De él depende absolutamente todo. Entonces, si esas tecnologías de seguridad no están con su esquema de alta disponibilidad, el negocio no va a funcionar. En ese sentido, hay tecnologías de seguridad en función de continuidad del negocio que son prioritarias. Y hay tecnologías que son suplementarias que no requieren del tema de contingencia. Si a nosotros se nos cae un antispam en un momento dado, no nos preocupa tanto. Sencillamente, tendríamos un período de eventual intromisión de spam o cosas de ese estilo pero no significa que el negocio se vaya a parar por esa razón.

Verónica Carreño

Desde la perspectiva de la prestación de servicios de continuidad, vemos en ocasiones barreras en la adquisición de herramientas que sirven para el manejo de continuidad del negocio. Una de ellas es en empresas



Verónica Carreño

pequeñas la falta de conocimiento de un esquema y de las políticas y procedimientos involucrados en el proceso sin contar aun la designación específica de personal que tenga como prioridad esta tarea. Cuando vamos a ofrecer de manera muy puntual una herramienta de continuidad de negocio tenemos que empezar con el levantamiento de información. Muchas veces tenemos que involucrar a un auditor o consultor que nos ayude en ese proceso.

En el caso de empresas con mayores alcances, la concientización y la disposición de recursos es mayor, pues generalmente se encuentran mecanismos ya establecidos es porque también ya tienen un esquema y unas herramientas que las siguen. Es aquí donde la cooperación con diferentes organismos de la misma organización se vuelve valiosa ya que ellos determinan los diferentes niveles de

criticidad de los recursos para la organización en general.

Carlos Baquero



Me voy a referir al cliente externo que son todas las personas del territorio nacional en la expedición de certificados judiciales y en la atención de asuntos migratorios del Aeropuerto Eldorado. Tenemos una contingencia bien importante y los esfuerzos que hemos hecho es precisamente garantizar la continuidad en ese tipo de servicios. Buscamos que la información que nos llega tenga un muy buen control de calidad y que esté bien salvaguardada.

Julio López

¿Cuál es la metodología comúnmente utilizada en su empresa para la definición del presupuesto asignado a las actividades de seguridad de la información? (actividades, fre-

cuencia, áreas participantes). ¿Cómo valora su organización los riesgos en seguridad de la información? (método, participantes, frecuencia). ¿Subdivide usted los riesgos en asegurable o no? ¿Tiene su organización seguros que la protejan en caso de ocurrencia de incidentes relacionados con su infraestructura informática?

Jaime Eduardo Santos

La metodología es alineación con el negocio dentro de un ejercicio presupuestal anual, con contratación y evaluación del desempeño y con la participación de la alta dirección y dentro de todo este proceso quien sustenta es la vicepresidencia de tecnología. Nuestra organización está orientada a las ventas y en todos los requerimientos de tecnología tienen prioridad los de ventas. A medida que se va diseñando lo que se va a vender se cuenta con la tecnología apropiada. Ese es el criterio de asignación en un ejercicio presupuestal en que todos nos comprometemos a que la utilidad del año va a ser X. y entre esa utilidad hay unas condiciones de inversión y de gasto. Con respecto a la pregunta seis nosotros trabajamos con un sistema integral de protección de riesgos en dos grandes sectores, los financieros en donde están los de cartera, de tesorería el otro sector son los riesgos operacionales de los cuales está el legal

tecnológico de la gente. La definición que tiene Basilea y para esta valoración de riesgos el lenguaje que procuramos utilizar es el de la NT 5254, la norma técnica 5254 porque una de las dificultades que encontramos en valoración es que hay quienes hablan de peligro, el otro habla de alarma el otro de amenaza y terminamos denominando el mismo aspecto de cinco maneras diferentes. Hace unos dos años venimos estandarizando el engranaje a través de esa norma. Con respecto al último punto no dividimos por riesgos asegurables o no porque como es un sistema integral de protección de riesgos se valora y dentro de esa valoración hay cosas que necesariamente son asegurables entonces eso no se debate. Eso simplemente hace parte de la póliza global bancaria o hace parte de la póliza de responsabilidad civil o hace parte de las políticas de protección de equipos o de caídas del sistema, se tienen todos los riesgos trasladados. Entonces ahí el tema para nosotros no es que se traslada, sino como se traslada y de que manera se es más eficiente en términos económicos en ese traslado. Entonces eso guarda relación si voy con un anexo en protección informática o voy con una póliza XXX. Si voy a cotizar en el mercado de Londres o en Estados Unidos o en los dos. Es una decisión financiera porque previamente hay una concepción de los riesgos que deben ser trasladados. Negociar es deducible.

Negociar los jaqueos, las visitas del sistema de auditoría, del sistema de revisoría. Es todo un tema gerencial en el que las pólizas deben estar pero tengo que ser eficiente en su administración.

Juan Carlos Huertas

Con respecto a la definición del presupuesto el Banco tiene una estrategia global en todo el Banco en particular con la subgerencia informática hay reuniones presupuestales anuales, nosotros estamos definiendo presupuesto alrededor de agosto o septiembre para el siguiente año. Ese presupuesto se conforma bajo dos parámetros. El primero de todas las áreas de la subgerencia informática reciben los requerimientos puntuales de todas las áreas del Banco. Y el otro nosotros trabajamos en función de generar oportunidades tecnológicas al negocio. Entonces son presupuestos originados dentro de las mismas áreas de la subgerencia. Este presupuesto es avalado a nivel de la gerencia ejecutiva, llega un nivel muy alto para justificar cada uno de los rubros que lo componen. También estamos sujetos a un proceso de racionalización del gasto, tenemos esa variable dentro de la estimación del presupuesto y también estamos desde este año trabajando con indicadores que miden la efectividad de la ejecución del presupuesto. En esto tenemos que ser mucho más agudos en determinar el presupuesto para el

año siguiente. Con relación al punto seis de cómo valora la organización los riesgos venimos desde hace muchos años trabajando con el estándar australiano, al que le hemos hecho una serie de adaptaciones porque una cosa es la teoría y otra la práctica. Ese es un poco el lenguaje, la manera de estimarlos. Pensamos que todas las metodologías de riesgo le apuntan a lo mismo. Hemos hecho una guía interna propia basada en este estándar y hoy en día hemos incluido un capítulo de BS 7799, nos estamos actualizando al 27001 y quienes participan en este sistema de riesgo que son todas las áreas del Banco en función de un grupo de riesgos que está ubicado dentro de la subgerencia. Se trata de un proceso anual; periódicamente se hace la generación de nuevos análisis de riesgos y también se hace revisión de análisis anteriores. Con respecto al punto 7 tampoco dividimos los riesgos en asegurables, todos están contemplados en la póliza global bancaria. En eso hemos trabajado bastante sobre todo lo que tiene que ver con seguridad. Antes las pólizas hablaban de virus, hoy en día logramos involucrar el código malicioso. Ahí podría haber un punto de fuga importante para la organización. La otra cosa que hemos logrado es haber podido incluir dentro de la póliza los riesgos relacionados con internet, tema relativamente nuevo y que normalmente no eran asegurados por las reaseguradoras. Otro

tema es que en el último caso de contratación de la reaseguradora se logró por motivación de ellos mismos que incluyeran un rubro dentro de la póliza que le obligue al Banco a través de la contratación de ellos a hacer ejercicio de vulnerabilidad tanto internos como externos. Eso es bueno para el Banco y para la aseguradora. Porque continuamente saben el estado en que está el Banco y las preocupaciones que deben atender.

Verónica Carreño

La pregunta seis. Como empresa multinacional cotizamos en la bolsa americana y tenemos que cumplir con una serie de requerimientos de cara a la información y a la infraestructura.

Tenemos dos mecanismos internos el primero a nivel de la infraestructura, este está relacionado con el nivel de recursos de servidores, hay una evaluación periódica, se han definido acuerdos de servicios y se presta como un servicio muy basado en la metodología interna de la parte de seguridad. El segundo está relacionado con respecto a los usuarios como había mencionando antes hay un mecanismo, unas políticas que contemplan que el usuario debe capacitarse entenderlas y certificarse en el tema.

Por otro lado también hay mecanismos que están monitoreando en todo momento las acciones del usuario y en que todas las políticas de seguridad se estén ejecutando, que el anti-virus esté actualizado, que las



El nuevo entorno de la seguridad informática ha abierto espacios para profesionales en disciplinas diferentes a la Ingeniería de Sistemas.

versiones de firewall estén actualizados que las contraseñas sean las adecuadas según políticas, que las versiones de sistemas operativos y sus fixes sean las adecuadas etc. Todo eso se está recogiendo y al final de cada año se da una calificación con base en el cumplimiento de las políticas. Todo eso se resume para un aseguramiento de la información.

A nivel de políticas de recuperación de la información también tenemos los mecanismos a nivel de infraestructura y se esta implementando en la actualidad un proyecto piloto en el que el respaldo de las estaciones de trabajo para cada usuario es responsabilidad de cada uno de ellos. Esto es responsabilidad de categorizar la información darle prioridad y mandar los respaldos a los servidores que están disponibles para este propósito. Entonces cada vez que sea necesario recuperar una máquina que no esté bajo el monitoreo de la infraestructura el usuario mismo tiene la posibilidad de recuperar su información.

Carlos Baquero

El método que utilizamos es la participación de todas las dependencias en donde se valoran las necesidades costo beneficio y de acuerdo con eso

se asigna el rubro para tales efectos. Eso se hace anualmente y se debe pasar una justificación bien sustentada para la tecnología y lo que se refiere a seguridad. Contamos con unos indicadores de gestión que nos muestran el estado de las cosas.

En otro sentido, nos enfocamos a la consultoría y asesoría del mismo talento humano. Contamos con un grupo de especialistas, ingenieros, analistas que están todo el tiempo actualizados con el tema de seguridad. Tenemos un banco de prueba que hace seguimiento al sistema y lo hace el mismo grupo. Somos conscientes de que es muy importante tener los sistemas actualizados y lo hace el área de sistemas. Yo pertenezco al área de delitos informáticos y participamos en eso porque formamos parte del comité. Velamos por esas conductas punibles sobre nuestros sistemas. De ese comité generamos un documento para socializar lo que encontramos en los sistemas y pasarlo a la gerencia. No enviamos eso al usuario común, solamente lo que tiene que ver con virus o cosas parecidas. Manejamos algunos seguros, algunas pólizas, pero como el tema también es nuevo, dichas pólizas no abarcan mucho que se ajuste a nuestras necesidades. A pesar de que esos aspectos no están tan fortalecidos, sí estamos trabajando en eso.