La seguridad en el Banco Central de México – Banxico –

Sara Gallardo M.

Entrevistamos a Jesús Vázquez Gómez, jefe de Seguridad Informática de la entidad.

El sector financiero es uno de los más expuestos a la delincuencia especializada en el delito relacionado con la información y los medios electrónicos. En Colombia, por ejemplo, se citan como fallas más frecuentes el software y los accesos a las páginas web no autorizados, además del código malicioso.

De ahí que la Superfinanciera, entidad que gobierna el ambiente bancario, avance en procura de los cambios necesarios para proteger la información y garantizar su seguridad.

La encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas –ACIS-, publicada en esta edición de la revista, señala en una de sus conclusiones que la inversión en seguridad de la información se concentra en las redes y sus componentes, así como en la protección de los datos de los clientes, aspectos directamente relacionados con los usuarios de las entidades bancarias.

De la investigación señalada, también se desprende la aparición de pólizas relacionadas con el cibercrimen, como un elemento emergente que se abre camino a nivel nacional y un nuevo control que motiva a las empresas de cualquier tamaño a revisar en forma permanente sus políticas y prácticas de seguridad.

Con el propósito de conocer los diferentes aspectos que atañen a la seguridad de la información, nos dirigimos a Jesús Vázquez Gómez, jefe de Seguridad Informática del Banco Central de México –Banxico-, quien respondió a nuestras inquietudes y describió el panorama del sector en su país, México.

RS: ¿Cómo define la seguridad dentro de la organización a la que usted pertenece?

JVG: La seguridad tiene dos enfoques, el denominado físico y el lógico. Ambos enfoques son cubiertos por áreas especializadas y cada vez se aprecia mayor cooperación e interdependencia entre ellas, por lo que la seguridad se define como el conjunto de controles que permiten gestionar el buen uso y la correcta operación de los sistemas de misión crítica en la organización.

RS: ¿Cuáles son los parámetros fundamentales en la que se sustenta?

JVG: Normatividad interna -políticas de seguridad-, controles administrativos, controles tecnológicos y un esfuerzo continuo por promover la toma de conciencia de los empleados respecto a la seguridad.

RS: ¿Cuál es el entorno jurídico que cobija la seguridad informática en su país?

JVG: Aunque aún incipiente, empieza a haber algunas regulaciones en materia de delitos cibernéticos, así como normatividad en aspectos como la clasificación de la información, transparencia en el acceso a la información, su resguardo, sanciones por uso no autorizado, entre otros.

RS: ¿Cómo asume el Banco al que usted pertenece la responsabilidad legal de su organización frente a los usuarios?

JVG: El Banco formula la normatividad interna a la que está sujeta todo usuario. Así, el usuario es responsable de los actos que conduzcan a afectaciones de la organización o de terceros. Si ocurriera algún incidente de tal naturaleza, pero se demuestra que el usuario actuó conforme a su manual de operación, normalmente no se le endilgarían responsabilidades.

El Banco formula la normatividad interna a la que está sujeta todo usuario. Así, el usuario es responsable de los actos que conduzcan a afectaciones de la organización o de terceros.

RS: ¿Qué tipo de seguros protegen al Banco ante cualquier eventualidad?

JVG: Los seguros que protegen ante eventualidades como incendios y otros daños materiales. El cubrimiento contempla inmuebles, equipos y software, en general. Se ha estudiado la posibilidad de asegurar la información crítica; sin embargo, es todavía un tema de investigación, sobre todo por el requisito de cumplir con estándares particulares, que no necesariamente se consideran adecuados o adoptables para el Banco.

RS: ¿Existe dentro del organigrama de su organización el cargo de gerente de seguridad de la información o solamente un directivo para el tema general de tecnología informática?

JVG: Actualmente la función de seguridad está inscrita bajo una Dirección General de Tecnologías de Información. Bajo ella existe la oficina de seguridad de la Información, que propone controles, genera políticas, asesora, y administra algunos controles propios de seguridad de la información.

RS: ¿Cuál es el perfil de ese directivo si lo hay?

JVG: De manera general se basa en los siguientes aspectos: estudios de postgrado en áreas de Ciencias de la Computación, Ingeniería en Sistemas o Ingeniería en telecomunicaciones; certificaciones: CISSP, CISA; conocimientos en Seguridad informática, Redes y Sistemas Operativos y Estándares; conocimientos básicos en: Normatividad Interna, Legislación;TOEFEL (+500); y, experiencia dirigiendo grupos de trabajo.

RS: ¿Existe una cultura empresarial en su organización frente al riesgo? ¿Cómo la abordan? ¿Cuáles acciones desarrollan en torno al tema?

JVG: Sí existe la cultura de manejo de riesgos informáticos, financieros, y operativos, entre otros. En los últimos dos años se ha realizado un esfuerzo para que la gestión del riesgo contemple los impactos a las diferentes áreas de negocio. Para sesionar y resolver situaciones de riesgo se ha constituido un grupo multidisciplinario.

RS: ¿La inseguridad es un tema que se aborda de manera directa o la estrategia del Banco se orienta solamente a partir de la seguridad? ¿Su banco contempla la gestión de la inseguridad?

JVG: Aunque la inseguridad no se considera de forma directa a nivel estratégico del Banco, sí se considera en el ámbito de la Oficina de Seguridad Informática a mi cargo, dado que cuando en el día a día se analizan riesgos o se evalúan posibles vulnerabilidades, es necesario pensar en cómo las cosas podrían ir mal. En ese sentido, la inseguridad no puede ser ajena a la forma de pensar de quienes somos responsables de los aspectos de protección o resguardo de la información de una institución.

RS: ¿Han sido objeto de casos específicos en los que el Banco haya tenido que responder de cara a la inseguridad informática?

JVG: Afortunadamente no ha habido casos en que el Banco, como organización, haya tenido que responder ante un descuido por no haber considerado el aspecto inseguridad. Internamente, desde luego que se presentan situaciones, aunque de menor impacto. Como en la mayor parte de la gestión informá-

tica, es muy posible que un estudio de inseguridad deba ser considerado desde el análisis de riesgos explícitamente.

RS: En casos así, ¿está previsto que responda la entidad y también quien maneja y dirige el área responsable del tema? ¿Cómo se define la responsabilidad para cada uno?

JVG: Dado que todos tenemos funciones definidas y procedimientos de operación, existe un área de control interno que lleva a cabo el deslinde de responsabilidades. Aunque para situaciones ante terceros afectados, el área jurídica se encarga de responder como organización, posteriormente de manera interna se determina la responsabilidad de algún empleado.

RS: ¿Existe una legislación específica de cara a las responsabilidades del gerente de seguridad de la información o de la persona al frente de la información?

JVG: Como responsables de una función en la Organización nos aplican las Condiciones Generales de Trabajo, la Ley Federal del Trabajo, así como las normas internas que pueden conducir a sanciones administrativas. Aunque no son específicas del cargo del responsable de la seguridad de la información.

RS: ¿Cuentan con un código de buenas prácticas de responsabilidad legal para la gerencia de seguridad? De ser así, ¿cuáles son los aspectos más importantes que lo componen?

JVG: No por ahora.

RS: ¿Cómo ve usted las tendencias y el futuro en estos temas?

JVG: Conforme los procesos críticos vayan siendo más dependientes de las tecnologías de información, deberán definirse más explícitamente las responsabilidades. Creo que deberán crearse áreas dedicadas a evaluar los riesgos de manera constante y no periódicamente -como ocurre ahora-, considerando en estas evaluaciones cómo las cosas pueden ir mal, generando la entrada para que las áreas de protección tomen las medidas más adecuadas sobre el entorno inseguro, que es demasiado dinámico. Por último, creo que la legislación informática vendrá prosperando en los próximos años para cubrir aspectos aún no desarrollados como son la evidencia digital, el proceso forense de datos y el trabajo a distancia, entre otras posibilidades.

Sara Gallardo M. *Periodista comunicadora, universidad Jorge Tadeo Lozano. Ha sido directora de las revistas Uno y Cero, Gestión Gerencial y Acuc Noticias. Editora de Aló Computadores. Redactora en las revistas Cambio 16, Cambio y Clase Empresarial. Corresponsal de la revista Infochannel (México). Autora del libro "Lo que cuesta el abuso del poder". Corresponsal en Colombia del Diario "La Prensa" de Panamá y revista IN de Lanchile; editora de esta revista y actual corresponsal de La Prensa Gráfica de El Salvador.*