



TOLERANCIA CERO FRENTE A LA INSEGURIDAD Y EL FRAUDE

Como estamos viviendo en los últimos meses, la seguridad en las entidades bancarias ha cobrado especial relevancia, ya que contribuye de forma muy importante a mantener la operatividad de la misma, aportando estabilidad al sistema financiero y preservando la confianza de los consumidores en las instituciones y órganos reguladores.

El control del fraude interno y del externo

El control del fraude interno y del externo ya no son conceptos abstractos, sino que han entrado de lleno a formar parte de los planes de negocio de las entidades, bien por lo establecido en las nuevas normativas, como los acuerdos de Basilea II, bien por las recomendaciones de las entidades reguladoras.

Para resolver los casos de fraude, las violaciones de políticas de seguridad o cualquier otro tipo de delito, los bancos deben contar con especialistas forenses, conocedores de las normas que regulan la actividad, capaces de obtener, preservar y presentar, de manera adecuada, la evidencia digital, así como de interactuar eficazmente con las autoridades judiciales.

Pero qué duda cabe que uno de los hechos más influyentes ha sido la sensibilización de la alta dirección, motivada por el conocimiento sobre el nuevo escenario al que nos enfrentamos, con inéditos canales financieros y una delincuencia cada vez más especializada y global, que se introduce hasta el fondo en las organizaciones. Véase el gran escándalo constituido por "el caso MADOFF".

En este contexto es claro que las entidades no son ajenas al aumento de los delitos que afectan al sector, y en especial a los asociados con un uso delictivo de las tecnologías de la información y las comunicaciones: robos de identidad, clonación de tarjetas, *phishing*, *pharming*, variantes *-ing* etc. Todos los mencionados se han convertido en términos que lamentablemente ya son noticia diaria en los medios de información general, con el consiguiente riesgo reputacional y pérdidas económicas asociadas.

Ésta es una poderosa razón por la que los bancos deben contar con directivos de seguridad visionarios e innovadores, con amplia experiencia en el mundo de la seguridad y conocedores del negocio, que vayan al menos un paso por delante de la delincuencia y que impulsen el desarrollo y la adopción de medidas de seguridad oportunas,

efectivas y acordes con los niveles de exposición al riesgo de las entidades y de sus clientes.

Estos frentes de actividad, formados en este nuevo escenario de operaciones, deben ser desarrollados por unidades altamente especializadas, capaces de entender los riesgos asociados a la operativa del banco, a la dinámica de los mercados, a la adopción de nuevas tecnologías y a la implementación de nuevos productos y servicios.

Explotación de las debilidades

Deben, además, tener las competencias necesarias para interactuar fluidamente con todas las áreas del banco, con proveedores de la entidad, con clientes y con entes externos, velando para que no se

lleguen a explotar las debilidades de los procesos de negocio y del sistema.

En armonía con lo dicho sobre las funciones de esta área de seguridad, y

Las entidades deben complementar su trabajo interno mediante la participación en grupos de trabajo, asociaciones sectoriales –a nivel nacional e internacional– y en foros que permitan compartir, con desprendimiento y sin prevenciones, conocimientos en materia de seguridad, vulnerabilidades, efectividad de los controles implementados, buenas prácticas adoptadas y resultados de la gestión de los riesgos, así como contar con repositorios de información especializados sobre el tema y bases de datos de eventos ocurridos dentro y fuera del país.

considerando que por mucho que nos esforcemos no será posible reducir el riesgo a cero, debemos estar preparados de la mejor manera posible, para hacerle frente a aquellos eventos que pudieran vulnerar la seguridad de la entidad.

Esto implica contar con especialistas forenses, conocedores de las normas que regulan la actividad, capaces de obtener, preservar y presentar, de manera adecuada, la evidencia digital, así como de interactuar eficazmente con las autoridades judiciales.

Dichos especialistas deben evaluar e

implementar herramientas y procedimientos con el fin de lograr procesos óptimos de investigación que permitan, realmente, resolver los casos de fraude, violación de políticas de seguridad o cualquier otro tipo de delito que pueda afectar a la entidad.

Estas actividades se deben complementar mediante la participación en grupos de trabajo, asociaciones sectoriales a nivel nacional e internacional y foros que permitan a los bancos compartir, con desprendimiento y sin prevenciones, conocimientos en materia de seguridad, vulnerabilidades, efectividad de los controles implementados, buenas prácticas adoptadas y resultados de la gestión de los riesgos, así como contar con repositorios de información especializados sobre el tema y bases de datos de eventos ocurridos dentro y fuera del país, esto es, participar en un análisis estratégico a nivel global. Porque "Lo que es, pues, de gran importancia en la guerra es combatir la estrategia del enemigo" (Sun Tzu, *El arte de la guerra*).

En definitiva, esta nueva estructura debe ser la encargada de definir unos estándares sobre los que construir su estrategia de seguridad, y dotar a la organización de instrumentos básicos para la adopción de medidas en permanente evolución, y ello, siempre apuntando a los más altos estándares sobre la materia, a las mejores prácticas,

y a la adopción de los procedimientos y los avances tecnológicos que ayuden a contrarrestar efectivamente la inseguridad, resumido en **tolerancia cero frente a la inseguridad y el fraude**. ■



José Antonio Lozano
Responsable de Seguridad Operativa

BANESTO