ASR Ltda.

NOTI INFORMATIVO

MAYO DE 2014

EDICIÓN No. 226

LA SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS DE FONDOS (2)

La gestión de los riesgos en las transacciones electrónicas debe desarrollar 5 tipos de acciones estratégicas, claramente diferenciadas.

Prevención: Orientada a reducir la posibilidad de ocurrencia de un evento indeseado. Igualmente se encarga de generar y mantener el ambiente ético adecuado. Ejemplos: manuales de procedimientos, políticas empresariales, capacitaciones.

De manera especial, debe impedirse el ingreso de personas no deseadas en la Organización. El proceso de selección, vinculación y monitoreo del personal al servicio de la empresa debe ser una actividad angular en la gestión de este riesgo; y debe involucrar, además de los departamentos de Recursos Humanos y las tradicionales evaluaciones de seguridad, elementos modernos que permitan no solo verificar el pasado y estilo de vida de las personas que van a ocupar cargos en la entidad, sino de manera especial y continuada la verificación del estilo de vida de los empleados, con el apoyo de las otras áreas de la empresa. Es importante tener en cuenta que solo un pequeño porcentaje de las personas que cometen fraude contra las empresas registran antecedentes penales.

Ello, debido a que en muy pocas ocasiones las víctimas deciden acudir a las autoridades para denunciar el hecho, bien sea porque están convencidas de la inoperancia de nuestro sistema judicial en este tipo de casos, que no siempre se pueden tipificar como delitos; o bien porque creen que pueden llegar a algún tipo de arreglo con el defraudador, quien se compromete a restituir las sumas apropiadas indebidamente, para luego defraudar, de nuevo, la confianza depositada en él.

Protección: Es el conjunto de acciones, elementos y equipos destinados a reducir las consecuencias de la materialización de un riesgo, tales como segregación de funciones, límites de autoridad, encriptación de información, clave de acceso, privilegios de

acceso al sistema de información, etc.

En el caso de las transacciones electrónicas, las medidas de protección resultan fundamentales, ya que por tratarse de actos no presenciales, cualquiera que posea las claves de acceso los puede realizar.

Las claves de acceso al sistema deben ser no solo seguras, sino personales y privadas. Una clave debe tener como mínimo 8 caracteres incluyendo al menos una mayúscula, un número y un carácter especial. Además de ser cambiada como máximo cada tres meses, debe elevarse a la categoría de falta disciplinaria grave el darla a conocer a otras personas, dentro o fuera de la organización.

Otra buena medida la constituye el dedicar un computador de manera exclusiva a la realización de transacciones, impidiendo que desde el mismo se acceda a la red o a otras páginas distintas de las de los bancos. Este computador debe dotarse de clave de acceso, antivirus y antimalware de última generación.

Por otro lado, deben establecerse topes de autoridad a los empleados para efectuar transacciones hasta un monto; y definir con los bancos los horarios en los cuales se pueden realizar transferencias.

Control: Son las acciones que permiten la detección temprana de la materialización de un riesgo, y las de combate del evento en su más temprana manifestación; tales como el análisis digital de información, las auditorías sorpresivas, y las pruebas automatizadas de auditoría.

Dentro de este grupo específico de acciones estratégicas conviene resaltar que el papel de control interno, auditoría o revisoría fiscal interna debe ser orientado a la consecución de tres objetivos claros:

- Verificar la efectividad de los mecanismos de control de riesgos de las diferentes áreas de la Organización. Es tarea fundamental del Control Interno el conceptuar si las estrategias de manejo de los riesgos que tiene implementada cada área o proceso se pueden considerar como Suficientes, Pertinentes y Coherentes.

- Hacer que las instrucciones de los directivos se acaten. Las áreas de control siguen siendo las llamadas a auditar de manera aleatoria pero sistemática el cumplimiento de los

procesos por parte de los empleados que los ejecutan; y,

- Generar valor. Los departamentos de control deben ser vistos en las organizaciones como verdaderos generadores de valor, al garantizar la correcta ejecución de las actividades de la empresa; lo que redunda en una mayor confianza por parte de accionistas, controladores, inversionistas y otros grupos externos e internos de interés.

Atención: Son aquellas acciones orientadas a manejar las situaciones que se generan por el descubrimiento o sospecha de un fraude. Se deben diseñar planes de Contingencia, para cesar el impacto de los eventos en los recursos, y planes de Continuidad, para recuperar la capacidad de operar en el menor tiempo posible.

· **Transferencia**: Existen dos maneras de transferencia: i) La transferencia del riesgo, por ejemplo cuando se contrata el transporte de dinero y valores con una firma especializada; o, ii) cuando se transfiere el efecto económico de la materialización de un evento, como en el caso de la contratación de seguros.

En la primera forma de transferencia, el riesgo queda a cargo de un tercero; en la segunda forma, se transfiere el efecto económico, pero la responsabilidad de administrar el riesgo físico continúa en cabeza de la organización.

asr@asr.com.co