Daniel Ramos Iglesias
Director General
SAFE Consulting Group

Fraude: un nuevo enfoque para combatirlo

Una de las mayores preocupaciones en Corporaciones y Sector Público en la actualidad es la necesidad de minimizar el impacto del fraude y la corrupción, incluyendo el Blanqueo de Capitales, en particular, en la gestión de operaciones, sin embargo y pese a ello, muchas entidades se ven sorprendidas por fraudes que nunca hubiesen imaginado. Esto se debe, a mi criterio, a una serie de debilidades desde el punto de vista estratégico y táctico en el planteamiento del combate contra el fraude corporativo que se podrían resumir en: inadecuado enfoque del combate al fraude, la carencia de una estructura dinámica de control, y en la deficiente utilización de tecnologías de detección disponibles y de bajo costo para combatirlo.

Inadecuado enfoque del Combate al Fraude: En primer lugar, muchas veces se observa que se ha planteado como un enfoque binario de sólo dos dimensiones –prevención y detección– que limita nuestra capacidad de reacción, sin embargo, "el enemigo" se encuentra en estado latente estudiando, preparándose y buscando el momento oportuno para dar el golpe, y si es posible, culpar a otro y escapar sin sospechas, de manera que el enfoque frente al fraude tiene que ser multidimensional, netamente creativo, a partir de una serie de estrategias que nos permitan desarrollar técnicas que ayuden a anticiparse a los hechos: estrategias pro-activas, de siembra, señuelos, limitación, reemplazo, alternativas forzadas, etc, que nos permiten dar a luz nuevos y diferentes enfo-

ques multidimensionales que tratarán de anticiparse al perpetrador o bien sorprenderlo, cebarlo, descubrirlo y capturarlo. Este cambio de enfoque que nos exige la máxima creatividad es esencial para alcanzar el éxito en la lucha contra el fraude.

Carencia de una estructura dinámica de Controles: El perpetrador de un fraude es una persona o peor aún un puede tratarse de un grupo de personas, motivada y que "gestiona su propio negocio", lo que bien podríamos llamar un emprendedor o *entrepreneur* que se enfrenta la mayoría de las veces en una lucha ventajosa y desigual contra una estructura y marco de control estático y vulnerable, en donde se pueden encontrar: rutinas de verificación repetitivas y controles "petrificados" durante años; sistemas que han sido reemplazados por paquetes externos con una importante pérdida de conocimiento sobre los nuevos procesos, y las tareas de control que antes se realizaban en forma manual y estaban perfectamente identificadas ahora quizás se encuentran en el mejor de los casos en manos de algún programa cuyo conocimiento está en manos del proveedor, unido esto a estructuras de control que o bien, se han externalizado o se han visto diezmadas por reducciones corporativas en donde ahora muchos procesos de negocios se encuentran en manos de proveedores que a su vez cuentan con personal muchas veces temporal, de elevada rotación y poca lealtad, sobre el que no tenemos ni de lejos el mismo nivel de control que antes de la externalización cuando los procesos eran internos, sumado esto a que los contratos externos tampoco contemplan en forma adecuada esta situación ni compensan los riesgos.

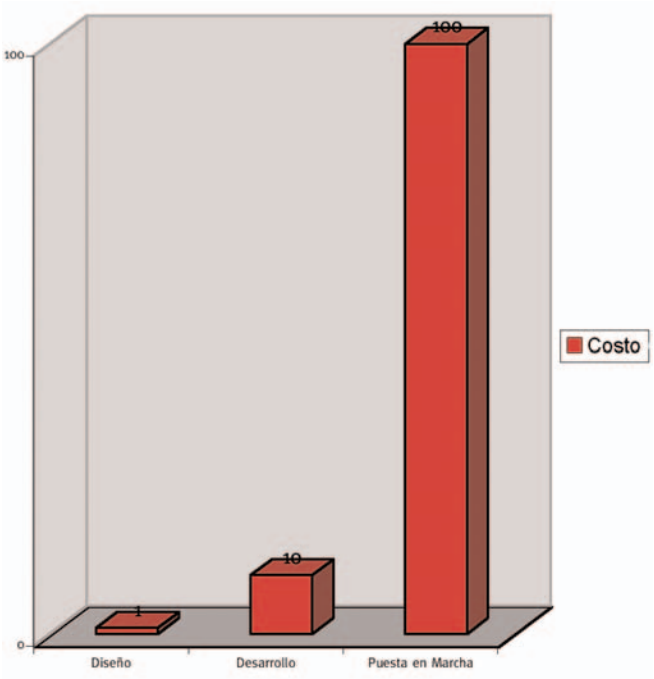
Deficiente utilización de Tecnologías para Combatirlo: Otro aspecto de gran relevancia y que también preocupa principalmente a los Consejos Directivos de muchas corporaciones a escala mundial –sobre todo a partir de los sonados casos de fraude reciente que han generado colapsos fulminantes en organizaciones tremendamente sólidas– es el tema del "Due Care", que podríamos traducir como "el debido cuidado" en el ejercicio de los negocios que toda empresa o entidad debería tener ya que podemos resumir la misión de buen Gobierno Corporativo de la Dirección en dos objetivos principales:

- Creación de Valor
- Gestionar los riesgos

Lamentablemente es muy común encontrar en la actualidad empresas y entidades públicas importantes en donde no existe –más allá de las áreas de Seguridad, Auditoria o Control- "conciencia de fraude" o al menos una actitud alerta y pro-activa de todo su personal respecto de este problema. En estos casos cuando se produce el problema y aún habiendo tenido la posibilidad de identificar y capturar al perpetrador, puede ocurrir que no se cuentan con los elementos mínimos desde el punto de vista legal para convencer a un juez de que la empresa ha gestionado y tenido el debido cuidado y de que existe la certeza (a prueba de toda duda razonable) respecto de que el perpetrador sea efectivamente el culpable. En este caso el gran problema es poder vincular a la víctima, la escena del delito, el perpetrador y los medios utilizados de manera que pueda establecerse la culpabilidad del perpetrador. Este problema se agrava sobre todo, frente a transacciones electrónicas en la medida en que el fraude se realiza en forma interna –donde en general no existen mecanismos de autenticación o firmas digitales– y muchas veces no está debidamente acreditada la responsabilidad, trazabilidad o auditabilidad del uso de las cuentas que identifican a los usuarios, ni tampoco se puede asegurar que las mismas no hayan sido utilizadas por otras personas no autorizadas.

Otro aspecto que se ha aprendido dolorosamente es que el coste de las inversiones en programas y medidas anti-fraude es de elevado retorno y que cuanto antes se implanten su coste resultará más reducido, como prueba de ello sólo basta mencionar este gráfico que refleja el costo de incorporar un control en los distintos estadios durante el desarrollo de una nueva aplicación (Ver Figura I).

Figura 1. Costo de incorporar un control en distintas etapas del desarrollo de sistemas



Es a partir de estas realidades, donde surge la necesidad de plantear una serie de contramedidas que permitan acotar el problema en forma integral.

Metodología para un Plan de Acción Global contra el Fraude

Como hemos visto el problema del fraude no puede atacarse con soluciones parciales, sino en forma integral, para lo cual, una adecuada metodología de análisis de riesgos orientado al fraude, resulta la de mayor efectividad para identificar los elementos de mayor vulnerabilidad corporativa y aplicar los recursos apropiados para atacar el problema.

Una adecuada metodología que logra identificar las vulnerabilidades del "negocio" (sea público o privado entendiendo como tal al objeto principal de las actividades) y establecer un ranking de procesos en relación al fraude, desmenuzando en detalle las vulnerabilidades y puntos de control, permite trazar un plan de acción preciso y alineado con los objetivos institucionales o de negocios, de manera que permita evaluar y comprender los riesgos, para establecer las técnicas y herramientas de control apropiadas para cada evento, o bien decidir si asegurar, transferir el riesgo remanente, o minimizarlo a partir de las múltiples dimensiones de las estrategias de control que mencionamos anteriormente.

Del reporte de Control Interno al proceso de Aseguramiento Continuo

Otra tendencia importante en materia de control es la de lograr que el "aseguramiento" del control –el rol fundamental de la Auditoría– debe ubicarse lo más cerca posible del origen del suceso, y no realizarse en forma "ex post" (como en la vieja historia que describe al auditor como aquel que va al campo de batalla luego de que la misma se ha perdido a contar los muertos y matar a los heridos; una imagen que por suerte ha cambiado donde el auditor se centraba en relatar lo que ha ocurrido con mínima posibilidad de recuperación de daños), sino con la nueva filosofía de bloquear la posibilidad de fraude o minimizar o recuperar el daño en caso de que ocurra. De esta forma del reporte de control interno vamos rápidamente aproximándonos al *Assurance* (aseguramiento) en línea, es decir implementando procesos no necesariamente en línea (lo que generalmente es muy costoso y sin mayor valor agregado sólo justificado en casos de transacciones con efecto inmediato y difícil recuperación) pero muy cerca del suceso, en función del riesgo o monto del proceso respectivo.

Diversos términos han permitido identificar el concepto de Aseguramiento Continuo, sin embargo, este proceso no debe confundirse con el de Monitorización Continuo o Sistema de Alertas, ya que ambos son diferentes componentes del proceso, como explicare en un momento.

Los elementos de un modelo de Aseguramiento Continuo son:

- Métricas (o mediciones de la realidad). Esto es recolectar información sobre los sucesos seleccionados tales como montos, fechas, consumos promedio, etc.

- Perfiles de contexto: contemplar los parámetros de la operación y establecer relaciones de parámetros en el mismo contexto, por ejemplo una factura en proveedor o ciudad determinada y en un día viernes.
- Comparaciones analíticas y de continuidad en el contexto: esto en particular se refiere a la relación de causa y efecto de un suceso con otro, por ejemplo un gasto en publicidad con un incremento de las ventas, así como las variaciones de los valores en un eje de tiempos y las demoras entre causa y efecto.
- Comparación con valores estándares: se trata de comparar lo que ocurre con parámetros máximos y mínimos, ya que sabemos que una compra no debería ser normalmente superior o inferior a tal cantidad.

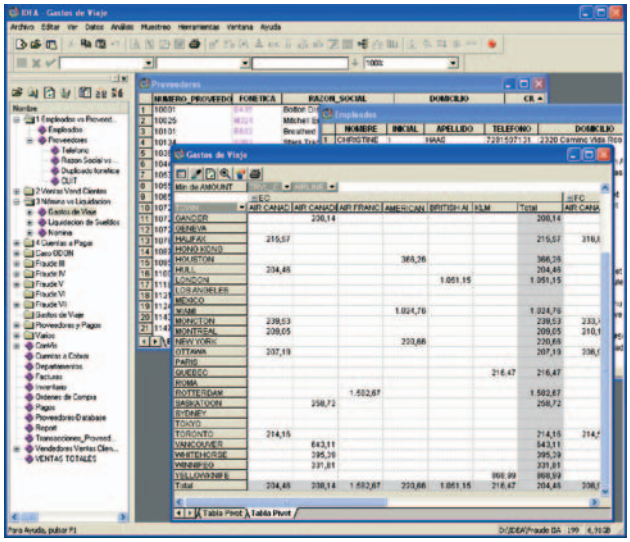
Este modelo utilizará comparaciones para determinar potenciales "indicios" de fraude, este proceso requiere una sintonía fina para ir acotando las alertas a los casos realmente excepcionales.

Tecnología de Análisis de Datos en Acción

El modelo se complementa con el uso creativo de herramientas especializadas para Análisis de Datos y Auditoría (como por ejemplo el Software IDEA que se muestra en el gráfico), que permiten explotar a fondo el potencial de los datos disponibles, para detectar indicios de fraude que luego generen rutinas y alertas en línea a partir del perfilado de los datos y la detección de parámetros excepcionales.

Además del análisis de rutina, también es muy importante la aplicación de pensamiento creativo para descubrir relaciones llamativas entre los datos que presenten algún indicio de fraude potencial. Un análisis típico es el de efectuar cruzamientos de datos que nunca se han comparado previamente en las aplicaciones que los procesan habitualmente, por ejemplo: Empleados versus Proveedores y verificar la existencia de contratas a nombre de empleados utilizando diversos medios de análisis. Además existen otras numerosas facilidades como por ejemplo, saber si alguna vez ha cambiado el precio de compra de un producto en todas las operaciones realizadas, o si algún oficial ha cambiado la tasa de préstamos para el mismo producto y sucursal, etc. Los análisis sólo se ven limitados por la creatividad del analista de fraude que los realiza, para luego recuperar el análisis y guardarlo como un programa automático que dispare las alertas en línea.

Vista de una herramienta de análisis de Datos (ej. IDEA).



Sin embargo, pese al potencial de análisis de estas herramientas puede ser necesario aplicar otras técnicas cuando sólo contamos con números y no tenemos mas información que nos permita identificar potenciales indicios de fraude. Es en estos casos en donde aplicamos el Análisis Digitalizado.

Análisis digitalizado - La Ley de Benford

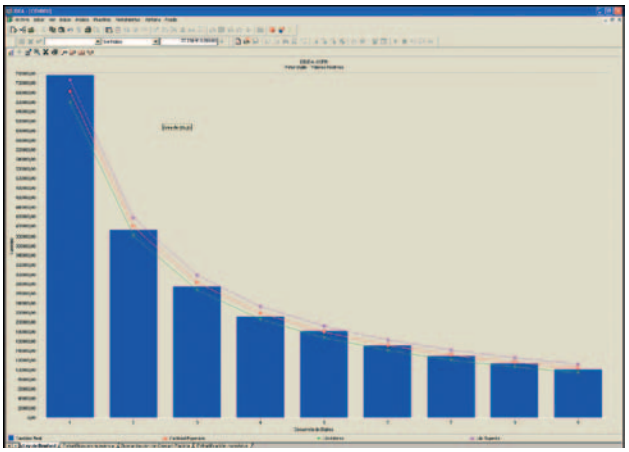
Por último, para no excedernos del espacio de este artículo, otra metodología muy utilizada es la conocida como Ley de Benford para análisis digitalizado. Para quienes no han escuchado hablar de él, Benford era un Ingeniero de General Electric que en 1920 observó que las tablas de logaritmos que se utilizaban para hacer cálculos estaban mas "usadas" en las primeras hojas respecto de las últimas, y lo mismo ocurría con las de sus compañeros de trabajo. En un momento de ocio creativo elaboró una hipótesis (de origen empírico–no científico) bastan-

te original, que indica que en un archivo de números hay más números que comienzan con 1 que números que comienzan con 9, pero más aún que los números de importes o cantidades en un archivo tienen una distribución determinada en función de sus primeros dígitos sin importar la cantidad de dígitos que tengan a la derecha. Esta distribución se representa con la fórmula

$$LOG_{10}(1 + 1/n)$$

Si usted aplica esta fórmula sobre los números 1 al 9, que son los dígitos con los que puede comenzar cualquier importe válido (no se computa el cero a la izquierda), comprobará que el 1 tiene una probabilidad del 30%, es decir que el 30% de los importes de un archivo comienzan con 1, y sólo el 4% comienzan con el número 9 (Ver Figura 2: Análisis del primer dígito de 2,3 millones de transacciones bancarias).

Figura 2. Distribución del primer dígito en un archivo de préstamos bancarios de 2,3 millones de casos

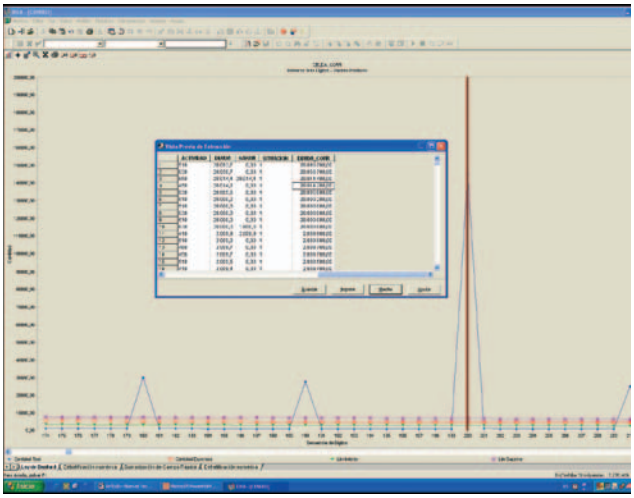


El hecho de conocer que los números auténticos y legítimos en un archivo cuentan con una distribución determinada permite inferir que los números fraudulentos o erróneos no responderán a esta distribución. Es más si un potencial perpetrador desea maximizar su fraude comenzando el importe de un pago o cheque con el número 9, tendrá una muy elevada probabilidad de ser detectado. Una de las bases del éxito de la ley de Benford es que "los delincuentes no la conocen", y desde ya confío en que los lectores de este artículo no se encuentran dentro de este grupo.

Como puede observarse en la Figura 2 –la distribución real (las barras verticales para el dígito 1 coinciden prácticamente con la distribución esperada las curvas por encima de las barras muestran la frecuencia esperada según Benford, los límites superior e inferior). Se sorprenderá al observar que esto es así en la mayoría de los archivos siempre que los importes o cantidades sean de datos homogéneos, y no incluyan comisiones, abonos o cargos fijos, los que deberán ser eliminados.

Sin embargo, la mejor parte del análisis es la de los tres primeros dígitos (Ver Figura 3) en donde realmente se obtiene un "electro-cardiograma" del archivo y podemos ver en detalle que está pasando en cada punto y cuáles son las transacciones con potencial fraude a fin de explorar detenidamente en cada una de ellas.

Figura 3 - Distribución de los tres primeros dígitos. Se observa el pico de 200 y los casos más significativos



Ahora donde la Ley de Benford adquiere real valor, es en la superposición de los mapas de incentivos para cometer un fraude con los picos observados en la distribución real de los números

sobre la distribución esperada por Benford. Por ejemplo en el control de las Compras sin Licitación o Compras Directas, la existencia de un importe límite que obliga a realizar una licitación o compulsa de precios es claramente un incentivo a cometer un fraude, ya que habrá quien divida una compra en importes menores para no tener que cumplir con el requisito de esta norma. En este caso Benford estaría indicándonos un pico llamativo inmediatamente antes del límite de compra indicándonos que hay más operaciones allí de las que debiera haber, por lo que accediendo a estas operaciones en detalle nos permitiría identificar específicamente las operaciones que presentan indicios de fraude y validarlas puntualmente. Adicionalmente podemos comenzar a explotar la información en este punto muchas veces identificando patrones respecto de meses, días de la semana, coincidencia con un nuevo proceso, nuevo empleado, vacaciones del responsable, mudanzas, etc.

La gran oportunidad

La tecnología nos presenta nuevos riesgos, pero también nos brinda una gran oportunidad. El más eficiente combate contra el fraude en la actualidad unido a una adecuada metodología y cultura organizacional, se logra con una metodología integral anti-fraude, y el uso de la tecnología en forma intensiva analizando universos completos de datos para identificar indicios de fraude y tomar acción sobre las mismas o bien disparar alertas en línea.

Sobre la base de la metodología indicada, el uso de una poderosa herramienta especializada de análisis de datos y auditoría orientada a la prevención y detección de fraude como IDEA se abren nuevos horizontes en esta lucha, y pone en las manos del experto en procesos operativos una herramienta de descubrimiento y creatividad, y de uso intuitivo para investigar, detectar y recuperar valor a partir de los datos corporativos analizando millones de registros de cualquier aplicación o base de datos, que también le permitirá automatizar sus procesos de Aseguramiento continuo y disparar las alertas necesarias, así como aplicar las facilidades de análisis digitalizado y cientos de funciones o prestaciones adicionales.

Esperamos que comparta estos nuevos enfoques y quedamos a su disposición para toda consulta o comentario adicional en info@safecg.com.