Galvanize

Detección y prevención de fraudes con estudios analíticos de datos

Tabla de contenidos

Detección y prevención de fraudes con estudios analíticos de datos 1

Los fraudes cuestan billones 3

Las herramientas de análisis de datos ahora son críticas 4

Por qué el muestreo ya no es suficiente 7

Tipos de pruebas de análisis 8

Avanzar hacia el monitoreo continuo 10

Técnicas de análisis de datos 11

- 01 Ley de Benford 12
- 02 Análisis de tendencias y de series temporales 13
- 03 Análisis de relaciones 14
- 04 Transacciones duplicadas 15
- 05 Importes enteros 16

Pasos para poner en marcha su programa antifraudes 17

20 pruebas comunes de estudios analíticos 18

Podemos ayudar con su programa de detección y prevención de fraudes. 23

Los fraudes cuestan billones

¿Sabía que los fraudes les cuestan a las organizaciones USD 2,1 billones por año a nivel mundial?[1] Para poner esa enorme cifra en perspectiva, ¡es más que el PIB total de Brasil, la octava economía del mundo!

Estas son otras cifras increíbles: el importe típico de pérdida de ingresos por fraude denunciado es del 5 %.[2] Esto significa que la estimación de pérdidas del sector de servicios de salud de EE. UU. (que tiene ingresos anuales de USD 3,5 billones) es de USD 175 000 millones, mientras que de los USD 1,2 billones de ingresos del sector de los seguros se pierden cerca de USD 60 000 millones.

No hay duda de que los mecanismos de fraude se han sofisticado y los defraudadores están constantemente buscando nuevas formas de manipular la tecnología en su beneficio. Las organizaciones y los gobiernos de todo el mundo están invirtiendo fuertemente en tecnologías y recursos para detener el flujo masivo de pérdida de ingresos.

Una de las tecnologías más valiosas para combatir el fraude son los estudios analíticos de datos avanzados. El software de estudios analíticos de datos puede identificar tendencias, patrones, anomalías y excepciones dentro de los datos y revelar las "huellas digitales" de los defraudadores.

En una encuesta reciente de PwC, el 44 % de los entrevistados respondieron que tienen previsto aumentar los gastos destinados a prevención de fraudes y delitos económicos en los próximos dos años.[3] El reporte dice que con la mayor parte de este dinero se financiarán tecnologías más potentes y estudios analíticos de datos.

Este libro electrónico analiza cómo implementar un programa exitoso contra los fraudes, incluye consideraciones y técnicas claves para la detección de fraudes y los tipos de pruebas que se pueden ejecutar, y da una serie de ejemplos prácticos que se pueden aplicar a una amplia variedad de funciones de negocios.

[1] **Deloitte,** *2018, Fighting fraud with analytics: The future of investigations (Combatir el fraude con estudios analíticos: el futuro de las investigaciones)*
[2] **Intel,** *2017, Stay ahead of fraud with big data analytics (Anticípese al fraude con estudios analíticos de big data)*
[3] **PwC,** *2018, Encuesta mundial sobre fraude y delito económico*

Las herramientas de análisis de datos ahora son críticas

La cantidad de datos que producimos en todo el mundo está creciendo y no hay señales de ralentización.

La International Data Corporation (IDC) definió tres áreas en las que se están creando datos:

01 El núcleo (centros de datos tradicionales y basados en la nube).

02 El borde (infraestructura comprobada en la práctica empresarial, como torres de telecomunicaciones y oficinas comerciales).

03 Las terminales (PC, teléfonos inteligentes y dispositivos de Internet de las cosas).

En conjunto, estos puntos de creación de datos conforman la "datosfera global", y se prevé que se pueda alcanzar la descomunal cifra de 175 zettabytes (ZB) en 2025.[4] Para poner este número en contexto, cada día, los usuarios de Internet producen 2,5 trillones de bytes de datos. Se necesitarían 400 días de recopilación de datos para llegar a un solo ZB. Y 70 000 días de navegación en Internet para llegar a 175 ZB.

Los datos crecen exponencialmente en todo el mundo —incluidos los datos de su propia organización— y eso hace que sea muy difícil descubrir los indicadores de fraude. Los controles internos por sí solos no son suficientes. (Y los empleados son cada vez más ingeniosos cuando se trata de encontrar formas de eludirlos).

Si quiere verificar y monitorear los controles internos con eficacia, debe recurrir a múltiples orígenes de datos, analizar el 100 % de las transacciones y verificar que todas cumplan con las políticas y los procedimientos establecidos en todas las aplicaciones y estructuras informáticas.

[4] **IDC,** *2018, The digitization of the world from edge to core (Digitalización del mundo desde el borde hasta el núcleo)*

Pero con volúmenes de datos tan enormes, revisar todo a mano es sumamente costoso y trabajoso —y básicamente imposible para las grandes organizaciones globales—. Sin embargo, con los estudios analíticos de datos, se tiene un panorama rápido de las operaciones de negocios y es fácil profundizar en los detalles de áreas específicas. Esto hace que los análisis sean más rápidos, más detallados y más exhaustivos que con los procesos manuales.

"El monitoreo proactivo de los datos se relacionó con un 52 % menos de pérdidas y los fraudes se detectaron en la mitad del tiempo".

» ***Asociación de Examinadores Certificados de Fraude,***
Reporte a las naciones 2018, sobre el fraude y el abuso ocupacional

CON LA ADECUADA TECNOLOGÍA DE ANÁLISIS DE DATOS, SE PUEDE:

+ Analizar automáticamente el 100 % de las transacciones en busca de indicadores de fraude.
+ Fusionar, normalizar y comparar datos de diferentes sistemas y orígenes.
+ Identificar rápidamente los fraudes antes de que se materialicen (o sean noticias de primera plana).
+ Realinear estratégicamente los recursos para concentrar los esfuerzos de detección en las transacciones sospechosas.
+ Calcular los impactos del fraude con mayor precisión.
+ Reducir significativamente los errores de muestreo y mejorar los controles internos.
+ Ahorrar tiempo mediante la automatización de las pruebas repetitivas.

¿QUÉ CARACTERÍSTICAS DEBE BUSCAR EN UNA HERRAMIENTA DE ANÁLISIS DE DATOS?

Estas son las cinco cosas que no pueden faltar en su solución de estudios analíticos de datos.

01 Capacidad de ejecutar rutinas analíticas prediseñadas como clasificación, estratificación, comprobación de duplicados, control de antigüedad, unión y búsqueda de coincidencias.

02 Capacidad de acceder y manipular datos, que permita acceder, comparar, depurar y combinar datos de casi cualquier origen.

03 Visualización de datos, para descubrir anomalías inesperadas con mayor facilidad y proporcionar información adicional.

04 Detección y prevención automatizadas, y desarrollo de pruebas complejas para detectar y enfrentar los tipos de fraudes más sofisticados.

05 Registro de procedimientos para generar las pistas completas de auditoría que pueden ser necesarias para respaldar las investigaciones detalladas.


ml

Por qué el muestreo ya no es suficiente

Muchos métodos para probar los controles, como el muestreo, presentan graves carencias.

- No es posible medir el impacto total de las fallas de los controles.
- Se pueden pasar por alto muchas anomalías menores —que, con el tiempo, pueden dar lugar a fraudes muy grandes—.
- Con pruebas por muestreo, no se encuentran patrones de advertencia ni se cumplen los requisitos normativos.

A pesar de que analizar muestras de datos es un enfoque de auditoría válido, no es tan eficaz a los efectos de detectar fraudes. Esto se debe a que las transacciones fraudulentas no suelen ser aleatorias.

Para probar y monitorear eficazmente los controles internos, las organizaciones deben analizar todas las transacciones relevantes; algo que es casi imposible sin estudios analíticos de datos y automatización.

Tipos de pruebas de análisis

En principio, hay dos tipos de pruebas de análisis de datos: ad hoc y repetitivas/continuas.

AD HOC

El objetivo de las pruebas ad-hoc es responder una pregunta de negocios específica. La prueba ad-hoc le permite explorar e investigar sus datos. Puede examinar las transacciones y ver si hay algo que indique que se ha cometido un fraude o identificar oportunidades para que se cometan fraudes.

Digamos que la dirección de un empleado coincide con la de un proveedor. Usted puede ir a buscar esa información específica: comparar el archivo maestro de proveedores con el archivo maestro de empleados y ver si hay registros coincidentes. Si encuentra algo, puede ser indicador de que alguien se configuró como proveedor fantasma. Con pruebas ad-hoc, se pueden descubrir oportunidades específicas en las que podrían cometerse fraudes.

Pero en realidad, sigue siendo manual y muy laborioso. Y, si ese tipo de anomalía parece ser relativamente prevalente o si usted no está cómodo con cierta exposición al riesgo, es posible que deba investigar de forma recurrente, lo que nos lleva al segundo tipo de pruebas.

REPETITIVO/CONTINUO

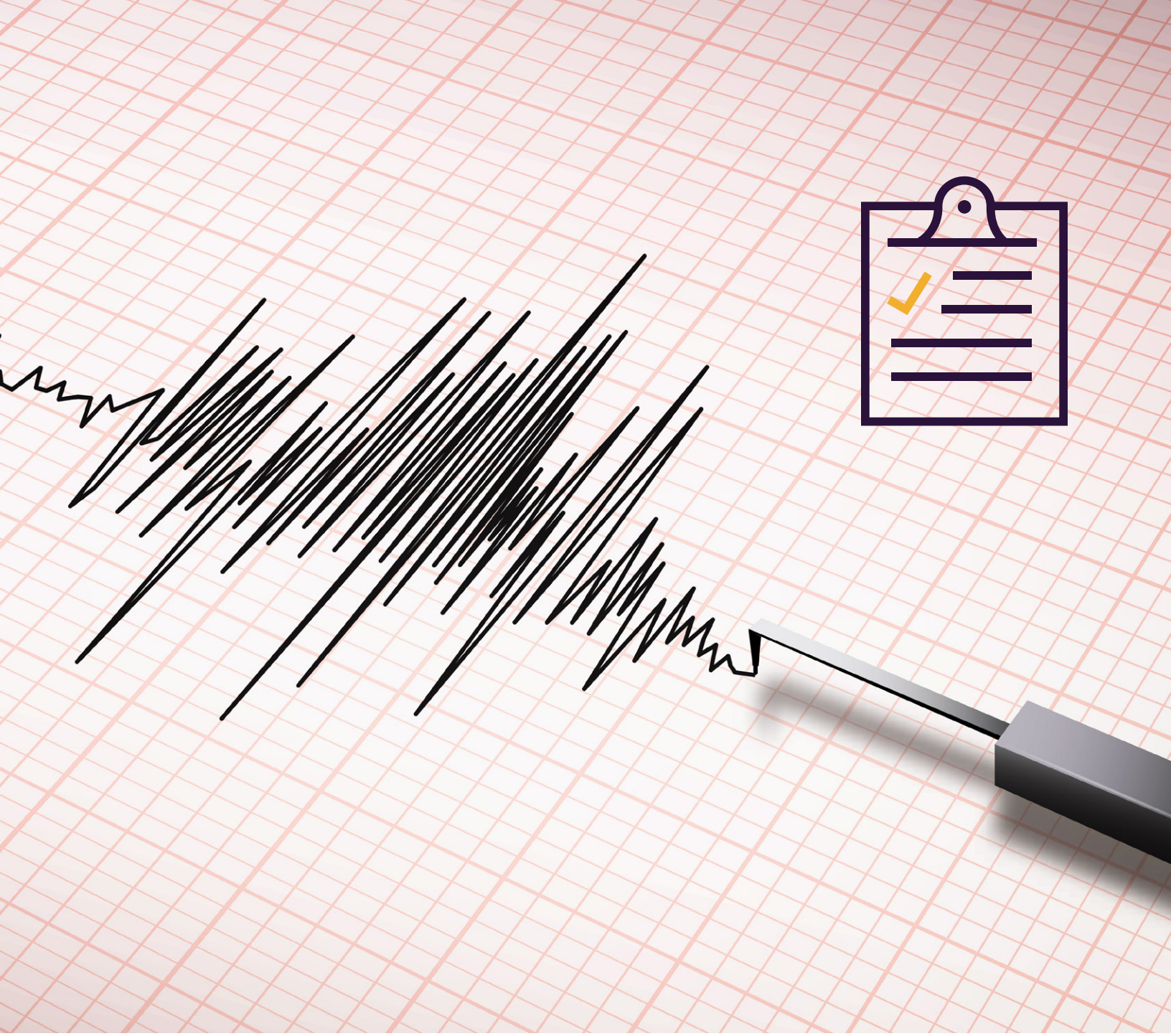
El análisis repetitivo o continuo para la detección de fraude implica configurar scripts que se ejecuten con grandes volúmenes de datos para identificar las anomalías en cuanto ocurren.

Este método puede mejorar en gran medida la eficiencia, la coherencia y la calidad generales del proceso de detección de fraudes. Crear scripts, probarlos y ejecutarlos con los datos para recibir notificaciones periódicas cuando se detecten anomalías.

Puede ejecutar el script todas las noches para revisar todas las transacciones y recibir notificaciones de las tendencias y patrones, y enviar las posibles excepciones a la gerencia. Comenzará a detectar la actividad fraudulenta tempranamente y de forma proactiva, antes de que las pequeñas anomalías se transformen en grandes problemas.

Por ejemplo, el uso abusivo de las tarjetas de compra (P-Cards) es un problema prevalente porque las grandes organizaciones suelen tener importantes volúmenes de compras con las P-Cards. Para enfrentarlo, se puede ejecutar un script que compruebe todas las transacciones de P-Cards cuando se generan, para asegurarse de que respeten los controles.

La automatización de las pruebas de problemas obvios como el de las P-cards le dejará tiempo libre para investigar otras áreas en las que podrían haber fallas o concentrarse en tareas y proyectos que requieren mucho tiempo y atención manual.



Estudios analíticos para el monitoreo automatizado de fraudes

El monitoreo automatizado de fraudes permite:

- Aplicar un enfoque basado en riesgos a sus programas de fraudes.
- Conectarse fácilmente a orígenes de datos internos y externos y automatizar el análisis para el monitoreo continuo.
- Aplicar estudios analíticos avanzados y técnicas de aprendizaje automático para identificar tendencias y actividades de alto riesgo.
- Marcar las infracciones, automatizar el seguimiento y notificar a las partes interesadas clave para combatir el fraude antes de que crezca.
- Refinar sus programas de estudios analíticos y monitoreo para centrarse en los fraudes de mayor riesgo y reducir los falsos positivos.

Avanzar hacia el monitoreo continuo

La Asociación de Examinadores Certificados de Fraude reportó que los casos típicos de fraude se prolongan durante 16 meses antes de ser detectados.[5]

Estas son ventajas obvias de la rápida detección de fraudes, y la oportuna mitigación de los riesgos es un argumento sólido para analizar y probar las transacciones de manera continua.

Una vez desarrollada la prueba para descubrir un indicador de fraude específico, es razonable repetir el análisis con regularidad. La frecuencia con la que se ejecutan las pruebas depende de sus metas y del tamaño de su organización. Por ejemplo, en el caso del monitoreo de transacciones de pagos e ingresos, podría ser conveniente ejecutar las pruebas automatizadas todos los días. En cambio, para áreas como los gastos de P-Cards, viajes y entretenimiento (T&E) y nómina, es posible que solo necesite realizar las pruebas una vez por semana o por mes, según la frecuencia de los pagos.

Pasar del uso ad-hoc de una suite de estudios analíticos de datos específicos para la detección de fraudes al monitoreo continuo es sencillo. Si asumimos que los temas del acceso a los datos y su preparación y validación están cubiertos, y que se ha verificado la eficacia de las pruebas, avanzar hacia el monitoreo continuo solo exige automatizar las pruebas.

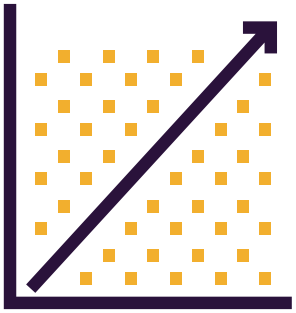
Luego, también se puede configurar un flujo de trabajo automatizado para las acciones correctivas. Las excepciones generadas por pruebas específicas serán automáticamente enviadas a individuos específicos para su revisión. Las notificaciones de excepciones de elementos de alto riesgo pueden enviarse a gerentes de más alto rango. Así, puede tener la certeza de que los problemas se señalan y se hace el seguimiento.

[5] **Asociación de Examinadores Certificados de Fraude,** *2018, Reporte a las naciones: estudio global sobre el fraude y el abuso ocupacional*

Técnicas de análisis de datos

Hay varias técnicas específicas de estudios analíticos de datos que son eficaces para la detección y prevención de fraudes.

01
Ley de Benford



La ley de Benford es una forma fascinante y muy eficaz de detectar fraudes potenciales y manipulación intencional de datos.

Es fascinante porque sorprende ver que las personas que inventan números o datos suelen seguir patrones y, en general, distribuyen los números uniformemente.

La ley de Benford es una técnica estadística común. Básicamente, establece que las listas de números de muchos orígenes de datos de la vida real se distribuyen de una manera específica y no uniforme. El número uno aparece cerca del 30 % de las veces. A continuación, el número dos aparece con menor frecuencia, luego el número tres, el cuatro, y así hasta el nueve (que aparece menos del 5 % de las veces). La idea es verificar ciertos puntos y números e identificar si aparecen con mayor frecuencia de la que deberían.

El análisis de datos permite encontrar puntos altos y bajos artificiales dentro de los datos, que podrían ser indicadores de fraude, y luego usted puede profundizar e investigar más.

La ley de Benford es particularmente útil para detectar fraudes de compras y cuentas por pagar. Otras áreas en las que su uso es adecuado son, entre otras:

+ Entradas de diario
+ Transacciones de cuentas por pagar
+ Reembolsos a clientes
+ Transacciones de tarjetas de crédito
+ Órdenes de compra
+ Datos de préstamos.

Ejemplo:
La ley de Benford puede aplicarse para determinar esquemas de fraude en los que los empleados estén adjudicando contratos por importes dentro de un cierto rango, en el cual un conjunto de números en particular (p. ej.: "39" en "39 000") aparece en los datos más de lo esperado. En este caso, el empleado podría estar adjucando contratos por debajo del límite de licitación y dirigiéndolos a una empresa con la que tiene un vínculo personal (p. ej.: un cónyuge o miembro de la familia).

02
Análisis de tendencias y de series temporales

El análisis de tendencias a lo largo de los años o en los departamentos, divisiones, etc. puede ser muy útil para detectar fraudes.

En resumen, el análisis de tendencias responde a la idea de que lo que sucedió en el pasado ayuda a saber qué sucederá en el futuro. En términos de datos, es una técnica estadística utilizada para calcular tendencias a lo largo del tiempo y hacer predicciones basadas en la hipótesis de que los patrones de la tendencia se mantendrán.

Con el análisis de tendencias, se puede examinar el balance del Mayor general a lo largo del tiempo. Cuando se tiene una expectativa de lo que va a suceder, se compara la tendencia con la expectativa. Si la tendencia no cumple con la expectativa de lo que va a suceder, se puede determinar por qué. El método del cambio de un período a otro es el tipo más simple de análisis de tendencias. Por ejemplo: usted proyecta datos hacia el futuro (un mes o un año) basados en datos de dos o más períodos anteriores y luego mide el resultado en dólares o porcentaje de cambio.

Ejemplo:

El análisis de tendencias es muy eficaz para detectar esquemas de sobornos. Por ejemplo, ejecutar un análisis de tendencias para comparar las tasas de devolución de productos defectuosos podría indicar un potencial esquema de comisiones ilícitas. En este ejemplo, alguien compra mercaderías de calidad inferior y las devuelve, recibiendo ganancias por una comisión ilícita. Los análisis de tendencias que observan cantidades y precios a lo largo del tiempo pueden revelar este tipo de fraude, especialmente en los casos en los que se compran significativamente más productos de los necesarios.

ANÁLISIS DE SERIES TEMPORALES

El análisis de series temporales es útil si los datos tienen un componente estacional (p. ej.: mayores valores asociados con determinados meses o días de la semana). El análisis predictivo a partir del análisis de tendencias y de series temporales puede usarse en un entorno de monitoreo continuo. El análisis puede ayudar a crear un pronóstico y luego pueden compararse esos datos con los reales inmediatamente después del evento. Cualquier diferencia entre ambos indica una divergencia de los datos con respecto a su tendencia anterior y significa que se ha producido algún cambio. Una investigación posterior podrá revelar si ese cambio fue intencional o malicioso.

03
Análisis de relaciones

Otra técnica útil para la detección de fraudes es el cálculo de relaciones en los campos numéricos claves.

Al igual que los ratios financieros que brindan indicadores de la salud relativa de una compañía, las relaciones del análisis de datos apuntan hacia posibles síntomas de fraude.

Tres relaciones comúnmente utilizadas son:

+ Mayor valor a menor valor (máximo/mínimo)
+ Mayor valor a siguiente más alto
+ Año actual a año anterior

En muchos casos, las relaciones altas o los valores anormales que se desvían del estándar del sector y/o de los escenarios actuales del negocio, suelen indicar fraudes potenciales que deben ser investigados.

04 Transacciones duplicadas

La prueba de duplicados es una de las pruebas de fraude más comunes porque puede indicar fraude además de ineficiencias o inexactitudes en las transacciones.

La ejecución de pruebas de transacciones duplicadas puede determinar, por ejemplo, que alguien está enviando facturas duplicadas, y si es deliberado o accidental.

Normalmente, las combinaciones de número de factura/número de proveedor son únicas. Por eso, las transacciones con la misma combinación de número de factura/número de proveedor serían un patrón de datos inesperado. Las transacciones duplicadas pueden ser un síntoma de fraude que debe examinarse. Pero, hay que tener precaución: es necesario investigar adecuadamente antes de sacar conclusiones apresuradas. Las transacciones que parecen duplicadas pueden ser simplemente pagos progresivos o facturas iguales por cargos mensuales.

Ejemplo:
Los números de factura duplicados pueden indicar que las facturas se pagaron dos veces, ya sea por accidente o intencionalmente. Un defraudador puede estar procesando esas facturas y pagándose el dinero a sí mismo, o trabajar con alguien de la empresa proveedora y compartir las ganancias de los pagos duplicados.

05
Importes enteros

Los importes enteros (redondeados a dólar) no suceden muy a menudo. Por eso, los números redondeados a decenas, cientos o miles pueden considerarse anomalías y deben estudiarse de cerca.

Y no se centre en los importes grandes. Los importes enteros pequeños deben revisarse, porque son los que usan generalmente los defraudadores para salir impunes. Por ejemplo, considere el reembolso de gastos de viaje. Su organización debe tener un importe diario máximo para viajes, comidas, gasolina, etc. Es muy probable que estos importes estén establecidos en valores enteros de dólares (p. ej., USD 90 para cenas, USD 200 por noche de hotel).

Para asegurarse de que no se superen esos máximos, las declaraciones deben compararse con los recibos. Por ejemplo, es muy poco común que el precio de una habitación de hotel sea a una cifra entera con los impuestos incluidos. Pero si tiene cientos de empleados que declaran gastos, serán miles los gastos para analizar y confirmar que los importes sean legítimos, y eso no puede hacerse a mano.

El análisis de datos permite que los usuarios identifiquen los importes de dólares enteros en los datos para poder investigarlos más y asegurarse de que las declaraciones coincidan con los datos.

Pasos para poner en marcha su programa antifraudes

La tecnología de análisis de datos puede ayudar a calcular el impacto del fraude para que usted pueda ver realmente cuánto le cuesta a la organización. Esto ayuda a determinar el ROI de la tecnología dedicada de estudios analíticos de fraudes.

- ☐ Escriba todos los tipos de fraude que podrían cometerse y las áreas en las que podrían ocurrir.
- ☐ Intente medir el riesgo de fraude y la exposición general de la organización. ¿Cuál sería el costo si realmente se cometiera el fraude que escribió en el primer paso?
- ☐ Atienda los elementos más costosos de la lista. Configure una prueba ad-hoc para buscar indicadores de fraude en esas áreas. Sobre la base de este análisis, investigue los patrones e indicadores que aparezcan y configure su monitoreo continuo.
- ☐ Comunique la actividad de monitoreo a toda la organización para que los empleados y los proveedores sepan que usted está prestando atención a lo que está sucediendo.
- ☐ Notifique inmediatamente a la gerencia cuando algo no marche bien. (Es mejor elevar los problemas rápidamente que explicar más tarde por qué sucedieron).
- ☐ Corrija de inmediato los controles que no funcionen. La división de tareas es importante. Si una persona puede iniciar una transacción, aprobarla y también recibir los bienes, allí hay un problema serio.
- ☐ Amplíe el alcance y repita.

20 pruebas comunes de estudios analíticos

¿Sabe cuánto le cuestan los fraudes? ***La tecnología de análisis de datos puede cuantificar el impacto del fraude.***

Las siguientes 20 pruebas exploran funciones de negocios en las que los fraudes son comunes, entre ellas: Mayor general, gastos de viajes y entretenimiento, nómina, informática, ciclo de compras y ciclo de ventas.

01 Entradas de diario sospechosas por palabras clave

Identifique descripciones sospechosas de las entradas de diario por medio de palabras clave que podrían indicar entradas no válidas o no autorizadas.

Ejemplo: Se encontró una descripción con la palabra clave "edificio" en la cuenta de activos a corto plazo. ¿Está mal clasificada? ¿Es válida?

02 Estratificación de cuentas del Mayor general

Estratifique una cuenta del Mayor general en particular para buscar entradas de diario fuera del rango normal de valores registrados en la cuenta.

Ejemplo: El promedio típico de las transacciones de gastos de nómina es de USD 2 millones, pero parece haber una entrada de USD 500 000, ¿es un registro debidamente autorizado?

03 Valores atípicos de entradas de diario

Seleccione entradas de diario que se desvíen por más de dos desviaciones estándares del importe promedio registrado.

Ejemplo: Analice las tendencias de todas sus cuentas para destacar las transacciones que pueden requerir un examen detallado. Estas transacciones son inusuales porque los importes son mucho mayores de los esperados.

04 Creación de perfiles de gastos

Cree perfiles de gastos mediante la identificación del gasto promedio por departamento.

Ejemplo: RR. HH. ha gastado grandes sumas en viajes de posibles candidatos y el personal del departamento de ventas ha volado en clase ejecutiva para viajes domésticos cortos.

05 Reclamos de reembolsos sospechosos: autos de alquiler, combustible y quilometraje

Identifique empleados que reclamen gastos de combustible cuando ya reclamaron gastos de quilometraje para sus vehículos personales, y reportes con gastos de combustible sin el correspondiente gasto de alquiler de auto.

Ejemplo: Tim presenta sus gastos de quilometraje cada semana por conducir su auto a ubicaciones fuera de la oficina. También ha presentado gastos de combustible para algunos de sus viajes, lo cual generó un error de reembolso que el equipo de finanzas no advirtió.

06 Compras divididas

Detecte las compras o gastos divididos del mismo empleado con la misma fecha y el mismo tipo de gasto, cada uno con un valor inferior al límite, pero que en conjunto superan el límite de aprobación.

Ejemplo: El límite de compras de Steve es de USD 500, pero él ordena nuevos suministros que cuestan USD 800 y divide la compra en dos pagos de USD 400. Cada pago está por debajo del límite, pero juntos superan el límite de aprobación.

07 Gastos excesivos de comidas grupales

Identifique los importes promedio por participante de las comidas grupales y reporte los casos que excedan los umbrales.

Ejemplo: Tony abusa de sus privilegios de T&E en las cenas de negocios y ordena USD 140 de alcohol por participante, muy por encima de su umbral autorizado de USD 50.

08 Importes redondeados

Identifique las transacciones potencialmente sospechosas con importes redondeados.

Ejemplo: Todos los meses hay una transacción misteriosa de Roger por USD 200. Ha estado haciendo un uso abusivo de su P-Card, retirando efectivo para uso personal.

09 Declaraciones duplicadas ("doble deducción")

Identifique empleados que estén creando declaraciones duplicadas ("doble deducción"), presentando el mismo gasto como una transacción de la tarjeta corporativa y una transacción pagada con recursos propios.

Ejemplo: Samara presenta declaraciones duplicadas por los mismos gastos; declara USD 360 por gastos de hotel en su tarjeta corporativa, pero también presentó otro reporte de gastos en el que declara que lo pagó con su tarjeta personal.

10 Tarjetas inactivas

Identifique las P-Cards perdidas, robadas o no utilizadas.

Ejemplo: Carol se fue de la empresa el año pasado, pero parece que su P-Card sigue activa en el sistema y aumenta el riesgo de exposición financiera.

11 Múltiples aumentos de salario

Identifique empleados con más de tres salarios base diferentes dentro de un mismo año, para asegurarse de que los aumentos sean válidos.

Ejemplo: Hay dos empleados que recibieron seis aumentos mínimos pero incrementales de salario durante el año anterior, ¿fueron aumentos autorizados?

12 Empleados fantasma

Identifique posibles empleados fantasma que se usen para fraudes (p. ej.: para canalizar fondos a una persona no autorizada).

Ejemplo: Un administrador de nómina ha reactivado empleados cesados y cambiado los datos bancarios por los de su propia cuenta.

13 División de tareas

Creación de facturas/proveedores.

Asegúrese de que exista una división de tareas entre quienes crean o modifican facturas y quienes crean o modifican proveedores.

Ejemplo: Julianna fue contratada como estudiante en prácticas a corto plazo. Pero su permiso de acceso al sistema nunca fue revocado y alguien puede usar su cuenta para crear facturas no válidas de proveedores ficticios.

14 Facturas duplicadas

Identifique posibles facturas duplicadas o pagos duplicados

Ejemplo: Un proveedor emitió accidentalmente facturas duplicadas para el mismo artículo, lo cual podría dar lugar a que se realizaran pagos duplicados.

15 Cambios frecuentes de campos sensibles en el archivo maestro de proveedores

Identifique los cambios frecuentes de campos sensibles en el archivo maestro de proveedores.

Ejemplo: La dirección de un proveedor se cambió a una ubicación no autorizada. Después del envío del cheque, la dirección volvió a corregirse.

16 Compras sin orden de compra

Identifique proveedores con transacciones sin orden de compra que superen un umbral especificado.

Ejemplo: Un proveedor presenta intencionalmente una factura falsa en connivencia con un empleado de la organización que comparte las ganancias después de aprobar y pagar la factura.

17 Coincidencia empleado-proveedor

Identifique las coincidencias entre la tabla maestra de empleados y la tabla maestra de proveedores para detectar errores de entrada o posibles fraudes.

Ejemplo: Se configuró una corporación ficticia para canalizar fondos a un empleado existente. La única información identificativa fue la coincidencia de los números de cuenta bancaria entre la información del empleado en la nómina y el archivo maestro de proveedores.

18 Recibos generales

Identifique recibos de compras por encima de cierto umbral en los que la mayor factura relacionada sea menor que un determinado porcentaje del recibo de compra.

Ejemplo: Se firma un acuerdo con una empresa de servicios por USD 100 000 de servicios de consultoría prestados en el curso de tres meses. Por desidia o deficiencias del proceso, el recibo completo por los USD 100 000 se ingresa de una vez. ¿Cómo garantiza que los servicios pagados fueron recibidos?

19 Validación de los límites de crédito de los clientes

Para asegurarse de que todos los límites de crédito asignados a los clientes respeten las políticas de la empresa, identifique a los clientes con límites de crédito inusuales o que no se hayan revisado durante un cierto período.

Ejemplo: A pesar de que su cliente GoodFood Inc. solo tiene autorizado un límite de crédito de USD 10 000, parece que se han aprobado pedidos por importes y cantidades mucho mayores. Esto representa una amenaza para su empresa por el riesgo de que GoodFood no sea capaz de pagar todos los bienes.

20 Clientes sancionados

Identifique clientes que estén en una lista de sancionados (lista de personas sancionadas de la Oficina de Control de Activos Extranjeros, lista de excluidos del registro de proveedores del Gobierno de EE. UU., lista de entidades e individuos excluidos de los programas federales de salud, etc.).

Ejemplo: Nicholas Vidall es un nombre destacado en la lista de personas sancionadas de la Oficina de Control de Activos Extranjeros por tener vínculos con miembros de un grupo de narcotraficantes. Las transacciones de ventas que involucren a este cliente deben revisarse a fondo antes de ser validadas.

Podemos ayudar con su programa de detección y prevención de fraudes.

Si desea una evaluación de cómo su organización puede integrar la tecnología de Galvanize para transformar el valor que genera su equipo, llame al 1 604 646 4254, envíe un correo electrónico a info@wegalvanize.com, o visite nuestro sitio web **wegalvanize.com**.

Galvanize

ACERCA DE GALVANIZE

Galvanize ofrece soluciones de software como prestación de servicios (SaaS) de gobernanza empresarial que ayuda tanto a gobiernos como a las empresas más grandes del mundo a cuantificar los riesgos, erradicar los fraudes y optimizar el desempeño.

Nuestra familia integrada de productos, incluyendo nuestra solución basada en la nube para gobernanza, gestión de riesgo y cumplimiento (GRC) y los productos insignia para análisis de datos, se utilizan en todos los niveles de la empresa para ayudar a maximizar las oportunidades de crecimiento mediante la identificación y mitigación de los riesgos, la protección de los beneficios y la aceleración del desempeño.

wegalvanize.com