Separata:

Modelo de detección de fraude en la administración pública

Autor: Dr. © Rafael Paredes Carrasco

La detección de fraudes es un proceso fundamental que implica la identificación de actividades sospechosas que podrían indicar un robo de dinero, datos o recursos. Este proceso suele ser facilitado por un software de detección de fraudes que monitorea transacciones, aplicaciones y comportamiento de los usuarios para identificar anomalías.

El fraude se manifiesta de diversas formas, como el robo de tarjetas de crédito, las estafas de inversión, el robo de cuentas y el blanqueo de dinero, con importantes consecuencias financieras tanto para las organizaciones como para la sociedad.

Para combatir el fraude de manera eficaz, especialmente a medida que se vuelve cada vez más sofisticado, las organizaciones recurren cada vez más a tecnologías avanzadas como los algoritmos de aprendizaje automático. Los sistemas tradicionales basados en reglas, aunque útiles, a menudo son insuficientes para detectar actividades fraudulentas más complejas. Los modelos de aprendizaje automático, como las redes neuronales y el aprendizaje automático, ofrecen capacidades mejoradas al analizar grandes conjuntos de datos e identificar patrones sospechosos que podrían pasar desapercibidos para los auditores humanos o los sistemas más simples.

Estos algoritmos aprovechan el big data, la nube y las técnicas de predicción modernas, lo que permite a las organizacións mejorar significativamente sus mecanismos de detección de fraudes.

Los modelos de predicción de fraude se clasifican en diferentes tipos, cada uno de los cuales atiende necesidades específicas en función de la naturaleza de los datos y el tipo de fraude que se aborda. Las características clave que se deben tener en cuenta en estos modelos incluyen datos transaccionales, análisis del comportamiento del usuario y patrones históricos de fraude. La evaluación de un modelo de predicción de fraude implica evaluar su precisión, exactitud y recuperación, entre otras métricas.

Las organizaciones están adoptando cada vez más el aprendizaje automático y la inteligencia artificial (IA) para la detección de fraudes, con un cambio notable desde los sistemas tradicionales basados en reglas a las aplicaciones de detección de

anomalías habilitadas con ML. Según la ACFE, una proporción significativa de organizaciones ya utilizan IA y ML para este propósito, y muchas más planean adoptar estas tecnologías en el futuro cercano.

Estos sistemas avanzados proporcionan un enfoque más dinámico y adaptable para la detección de fraudes, aprendiendo continuamente de nuevos datos y evolucionando para contrarrestar las tácticas de fraude emergentes.

Métodos de prevención del fraude

Los métodos de prevención del fraude abarcan una variedad de enfoques diseñados para crear una defensa sólida contra las actividades fraudulentas. Estos métodos incluyen análisis avanzados de datos, que analizan grandes conjuntos de datos para identificar patrones y anomalías indicativas de fraude. Las auditorías internas y externas sirven como exámenes sistemáticos de los registros y operaciones financieras para garantizar la precisión y el cumplimiento de las leyes y regulaciones. Además, las investigaciones de las fuerzas del orden son cruciales para descubrir y abordar esquemas fraudulentos que pueden extenderse a varias jurisdicciones. Los programas de denuncia de irregularidades también desempeñan un papel importante, ya que brindan un mecanismo para que los informantes internos denuncien actividades sospechosas sin temor a represalias.

En conjunto, estas estrategias forman un mecanismo de defensa de múltiples capas que es esencial tanto para los gobiernos como para las organizacións para combatir eficazmente el fraude.

Técnicas de análisis de datos

Las técnicas de análisis de datos se han vuelto indispensables en el ámbito de la detección, prevención e investigación de fraudes. Estas técnicas permiten a las organizaciones identificar anomalías y patrones dentro de conjuntos de datos complejos, que son cruciales para mitigar las actividades fraudulentas.

En los últimos años, los métodos tradicionales de detección de fraudes, como las auditorías manuales, han demostrado ser insuficientes para abordar la naturaleza sofisticada y rápidamente cambiante del fraude. Los sistemas manuales suelen ser demasiado lentos e inflexibles y las tácticas fraudulentas modernas pueden burlarlos fácilmente. Esta brecha se ha cubierto de manera eficaz con el análisis predictivo, que aprovecha los datos, el aprendizaje automático y los algoritmos avanzados para

identificar y neutralizar de manera proactiva las posibles amenazas de fraude antes de que causen daños significativos.

Los modelos de análisis predictivo, las técnicas avanzadas de aprendizaje automático y las fuentes de datos alternativas desempeñan un papel fundamental en la prevención del fraude. Estas tecnologías analizan grandes cantidades de datos para identificar patrones y anomalías que indiquen un comportamiento fraudulento, lo que permite a las organizaciones tomar medidas rápidas y adecuadas.

Según la Asociación de Examinadores de Fraude Certificados (ACFE), el análisis y monitoreo de datos proactivos se encuentran entre los controles antifraude más efectivos. Las organizaciones que implementan estas técnicas experimentan incidentes de fraude significativamente menos costosos y detectan el fraude mucho más rápidamente en comparación con aquellas que no emplean dichos métodos. Los procesos y técnicas de análisis de datos proactivos pueden identificar sistemáticamente señales de alerta y realizar modelos predictivos, a menudo descubriendo el fraude mucho antes de que lo hagan los métodos de investigación tradicionales.

Aprendizaje automático en la detección de fraudes

El aprendizaje automático ha surgido como una herramienta fundamental en el ámbito de la detección de fraudes, ya que aborda las limitaciones de los sistemas tradicionales basados en reglas al ofrecer técnicas avanzadas para identificar y predecir actividades fraudulentas. Los métodos tradicionales a menudo no reconocen patrones complejos y no pueden adaptarse a nuevas tácticas de fraude, y es ahí donde el ML se vuelve invaluable.

Los algoritmos de aprendizaje automático, incluidas las redes neuronales y el aprendizaje automático, son excelentes para analizar grandes conjuntos de datos y detectar anomalías que la supervisión humana podría pasar por alto.

La capacidad del aprendizaje automático para procesar y aprender de grandes cantidades de datos garantiza un enfoque más dinámico y adaptativo para la detección de fraudes.

Las ventajas de utilizar el aprendizaje automático para la detección de fraudes son múltiples. Estos sistemas pueden analizar rápidamente grandes conjuntos de datos para identificar patrones irregulares, mejorando así las capacidades predictivas a lo largo del tiempo.

Además, las organizacións recurren cada vez más al aprendizaje automático y a la inteligencia artificial (IA) para abordar diversas formas de fraude, como el fraude en los pagos, el robo de identidad y la apropiación de cuentas.

Este cambio subraya la creciente dependencia de estas tecnologías por su adaptabilidad y precisión.

Una parte importante de las organizaciones ya han adoptado o planean adoptar IA y ML para la detección de fraudes, reconociendo las capacidades mejoradas que ofrecen estas tecnologías en comparación con los métodos tradicionales.

Esta tendencia está impulsada por la necesidad de mantenerse a la vanguardia de los esquemas fraudulentos sofisticados que evolucionan continuamente con los avances tecnológicos.

Para garantizar la eficacia continua de los modelos de aprendizaje automático a medida que evolucionan las tácticas de fraude, es esencial actualizarlos periódicamente con nuevos datos y perfeccionarlos en función de los patrones de fraude más recientes. Las mejores prácticas incluyen el seguimiento continuo, el reentrenamiento de los modelos con datos actuales y la incorporación de ciclos de retroalimentación para mejorar la precisión y la adaptabilidad del sistema.

Al adherirse a estas estrategias, las organizacións pueden mantener una defensa sólida contra las amenazas de fraude en constante cambio.

Evolución de las auditorías internas con los avances tecnológicos

El papel de las auditorías internas en la detección y prevención del fraude está evolucionando significativamente con los avances tecnológicos, en particular la inteligencia artificial (IA) y el aprendizaje automático . Las instituciones de educación superior, entre otros sectores, buscan cada vez más formas de ganar eficiencia en sus procesos debido al cambiante entorno operativo y a los desafíos políticos y económicos.

La introducción de tecnologías como los transformadores generativos preentrenados (GPT), ejemplificados por el lanzamiento público de ChatGPT, marca un cambio fundamental en el panorama de la auditoría interna.

Se espera que las tecnologías emergentes como la IA, el aprendizaje automático y la cadena de bloques den forma al futuro de la auditoría.

Estas tecnologías prometen mejorar la eficiencia, mejorar la calidad de la auditoría y reducir los costos a largo plazo, lo que presenta un potencial transformador para los departamentos de auditoría interna.

Sin embargo, esta transformación también conlleva riesgos, incluidas preocupaciones sobre la privacidad de los datos e incertidumbres sobre el retorno de la inversión.

La adopción e integración efectivas de estas tecnologías requieren una gobernanza sólida, una participación reflexiva de las partes interesadas y una planificación estratégica.

La evolución de las auditorías internas con estos avances tecnológicos también plantea importantes implicaciones éticas y profesionales. Los auditores deben prepararse para las nuevas habilidades y competencias que requiere la auditoría de próxima generación.

A medida que la inteligencia artificial y el análisis de datos transforman las auditorías internas, resulta crucial desarrollar nuevas estrategias para adoptar e integrar eficazmente estas tecnologías.

Esta transformación es esencial no sólo para mejorar la eficiencia sino también para mejorar las capacidades de detección y prevención de fraude en un entorno operativo cada vez más complejo.

El papel de las auditorías externas con herramientas de aprendizaje automático

Las auditorías externas desempeñan un papel fundamental en la detección y prevención del fraude, y la aparición de herramientas de aprendizaje automático ha mejorado significativamente su eficacia. Los algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos para identificar patrones y anomalías que las revisiones manuales tradicionales podrían pasar por alto. Esta tecnología es particularmente eficaz para realizar pruebas de entradas de diario al identificar transacciones inusuales dentro de grandes grupos de datos no estructurados, que luego se analizan en busca de posibles indicadores de fraude.

Durante la fase de planificación de la auditoría y mientras se realizan los procedimientos de identificación y evaluación de riesgos, el aprendizaje automático se puede utilizar para procesar cantidades sustanciales de datos, como extractos bancarios y contratos legales, de forma mucho más rápida y precisa que los auditores humanos. Al automatizar estos procesos, el aprendizaje automático reduce la probabilidad de error humano y aumenta la eficiencia de la auditoría.

El aprendizaje automático también revoluciona la evaluación de riesgos y la detección de fraudes en el ámbito de la auditoría, ya que permite a los auditores ir más allá de las técnicas de muestreo tradicionales, que suelen requerir mucho tiempo y ser propensas a errores. En cambio, el aprendizaje automático puede realizar un análisis exhaustivo de todos los datos disponibles, lo que proporciona una evaluación más exhaustiva de los posibles riesgos y actividades fraudulentas.

Esta capacidad mejorada permite a los auditores identificar esquemas de fraude sofisticados que de otro modo podrían pasar desapercibidos, mejorando así la calidad y la confiabilidad generales de la auditoría.

Impacto en la rentabilidad

El fraude puede tener efectos perjudiciales significativos en la rentabilidad de una organización. Según el "Informe a la Nación 2012" de la Asociación de Examinadores de Fraude Certificados (ACFE), una organización típica pierde aproximadamente el 5 por ciento de sus ingresos anuales debido a actos fraudulentos.

Estas pérdidas financieras se ven agravadas por el impacto negativo a largo plazo en la reputación y los objetivos financieros de una organización.

Mantener la confianza y la integridad en el lugar de trabajo es esencial para el éxito y la sostenibilidad de cualquier organización. El fraude en el lugar de trabajo, que incluye actividades como malversación de fondos, soborno, falsificación de registros y tráfico de información privilegiada, puede socavar esta confianza y afectar a toda la organización.

Por lo tanto, las organizaciones deben considerar seriamente el riesgo de fraude y tomar medidas proactivas para mitigar estos riesgos.

La integración de análisis de datos avanzados puede ser una herramienta poderosa para identificar y prevenir actividades fraudulentas, protegiendo así la rentabilidad de la organización.

Mitigación de impactos con análisis de datos avanzados

El fraude puede tener consecuencias de gran alcance que ponen en peligro todas las áreas de la organización. La reacción inicial al fraude suele centrarse en las pérdidas financieras, pero esta mentalidad no reconoce su impacto general, incluidas las implicaciones para los clientes, la reputación, las operaciones y los ingresos.

Se considera erróneamente que el fraude es un delito sin víctimas, pero puede tener efectos sociales y psicológicos considerables en las personas, las organizaciones y la sociedad. Drena recursos, afecta a los servicios públicos e incluso puede financiar otras actividades delictivas y terroristas.

El impacto del fraude en las organizaciones puede ser devastador y provocar pérdidas financieras significativas, daños irreparables a la reputación, posibles repercusiones legales y una disminución de la moral y la confianza de los colaboradores.

La integración de análisis de datos avanzados puede ayudar a mitigar estos impactos. Al comprender la totalidad de las diversas implicaciones que surgen del fraude, los comerciantes pueden desarrollar estrategias más efectivas para abordar las cargas financieras tanto directas como indirectas. El análisis de datos avanzado permite a las organizaciones detectar patrones y anomalías que pueden indicar una actividad fraudulenta, mejorando así la capacidad de prevenir el fraude antes de que ocurra. Este enfoque proactivo no solo salvaguarda los activos financieros, sino que también protege la reputación y la integridad operativa de la organización. El uso de herramientas de análisis sofisticadas permite a las organizaciones implementar controles internos sólidos y administrar mejor su fuerza laboral, reduciendo así las posibilidades de incidentes de fraude importantes.

Principales desafíos que enfrenta la aplicación de la ley

Las fuerzas del orden se enfrentan a numerosos desafíos en la investigación de casos de fraude, que se derivan de la complejidad de las transacciones financieras, los métodos sofisticados empleados por los defraudadores y la necesidad de conocimientos especializados en contabilidad y análisis forenses digital.

Las complejidades del fraude financiero a menudo requieren que las agencias cuenten con las herramientas y los procedimientos necesarios para responder de manera eficaz, incluido un conocimiento profundo del proceso de investigación financiera.

Un desafío importante es la pérdida de datos debido a cambios legislativos como el Reglamento General de Protección de Datos (RGPD), que puede limitar el acceso de las fuerzas del orden a información crucial.

Además, el creciente volumen de datos generados por los avances tecnológicos y el uso generalizado de Internet dificulta que los investigadores identifiquen a usuarios específicos involucrados en actividades fraudulentas.

El anonimato que proporcionan las tecnologías de la información y la comunicación complica aún más las investigaciones, ya que los ciberdelincuentes utilizan técnicas como servidores proxy para ocultar sus identidades y actividades.

Este anonimato puede dificultar considerablemente la capacidad de las fuerzas del orden para rastrear y detener a los perpetradores.

La ciencia forense digital desempeña un papel fundamental en las investigaciones de delitos cibernéticos, pero presenta sus propios desafíos. Mantenerse al día con los rápidos avances tecnológicos y abordar las cuestiones legales y éticas son problemas constantes para los expertos en ciencia forense digital.

A pesar de estos obstáculos, los esfuerzos de colaboración con otros organismos encargados de hacer cumplir la ley son esenciales para superar estos desafíos, ya que permiten compartir conocimientos, recursos y experiencia que son fundamentales para el éxito de las investigaciones y los procesamientos.

Dificultades en la investigación de casos de fraude

La investigación de casos de fraude dentro de los gobiernos presenta varios desafíos importantes. Uno de los principales problemas es la falta de una definición uniforme de fraude en las distintas agencias, lo que dificulta el estudio y la comparación exhaustiva de los datos relacionados con el fraude.

Esta variabilidad en las definiciones complica los esfuerzos por estandarizar la recopilación y el análisis de datos.

Además, la naturaleza intrínsecamente engañosa del fraude implica que a menudo no se detecta ni se denuncia. Esta falta de denuncia genera lagunas en los datos, lo que dificulta la capacidad de los organismos para medir el verdadero alcance de las actividades fraudulentas.

Los datos existentes sobre el fraude suelen ser incompletos e inconsistentes, lo que dificulta aún más las investigaciones y los análisis exhaustivos.

A pesar de estos desafíos, existen recursos disponibles para ayudar a combatir el fraude dentro del gobierno. Por ejemplo, los recursos antifraude en línea brindan herramientas e información valiosas para ayudar a las agencias en sus esfuerzos de detección y prevención.

Desafíos de los algoritmos de aprendizaje automático para la detección de fraudes

El desarrollo y la implementación de algoritmos de aprendizaje automático para la detección de fraudes plantea varios desafíos importantes. Uno de los principales problemas es el problema predominante del desequilibrio de datos, que surge de la distribución desigual de transacciones fraudulentas y no fraudulentas dentro de los conjuntos de datos.

Este desequilibrio puede obstaculizar significativamente el rendimiento de los modelos de aprendizaje automático, ya que pueden volverse parciales hacia la clase mayoritaria, lo que genera una mayor tasa de falsos negativos.

Otro desafío importante es la necesidad de eficiencia computacional. Garantizar que los modelos de conjunto puedan manejar algoritmos complejos, ingeniería de características intrincadas y la integración de diversos modelos base sin comprometer la velocidad es crucial para una detección eficaz del fraude.

La naturaleza rápidamente evolutiva del fraude digital requiere que estos modelos no solo sean precisos sino también rápidos para adaptarse a nuevas técnicas de fraude.

Los métodos tradicionales basados en reglas a menudo pasan por alto patrones complejos y no pueden predecir nuevas tácticas de fraude, lo que los hace menos efectivos contra esquemas de fraude sofisticados.

Sin embargo, los modelos de aprendizaje automático deben evolucionar constantemente para reconocer patrones de fraude nuevos y emergentes, lo que requiere un aprendizaje y una actualización continuos de los modelos. Esta adaptabilidad es esencial para mantener sistemas de detección de fraude robustos.

Además, la implementación de algoritmos de aprendizaje automático para la detección de fraudes también implica abordar ineficiencias operativas, posibles pérdidas financieras, pérdida de confianza de los clientes y daño a la reputación.

Hay mucho en juego, ya que no detectar con precisión el fraude puede tener consecuencias jurídicas importantes y erosionar la confianza en las instituciones.

Por último, la integración de algoritmos avanzados de aprendizaje automático en los marcos de detección de fraude existentes puede ser un proceso complejo. Las organizaciones deben asegurarse de que estos algoritmos sean escalables y capaces de analizar grandes cantidades de datos en tiempo real, lo que puede resultar técnicamente exigente.

La capacidad del aprendizaje automático para predecir y prevenir actividades fraudulentas antes de que ocurran subraya su potencial como herramienta poderosa en la lucha contra el engaño digital.

Bibliografía

- Guía Señales de Alerta Indiciarias de Lavado o Blanqueo de Activos para el Sistema Financiero y Otros Sectores. Unidad de Análisis financiero. 2010.
- Ley 20.393 - Establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica.
- Oficio FN N° 440/2015 del 23.08.10 Instrucción General que imparte criterios de actuación para la investigación y persecución penal de las personas jurídicas. Fiscalía.
- Tipologías regionales GAFISUD. Grupo de trabajo de Unidades de Inteligencia Financiera – GTUIF. 2008.
- Tipologías y Señales de Alerta de Lavado de Activos en Chile. Unidad de Análisis financiero. 2013.