Faro de Auditoría

Boletín Flash del Comité Latinoamericano de Auditoría Interna (CLAIN)

FELABAN

No.19 –Abril 2017

Aplicando "analytics" en la batalla contra el fraude en instituciones financieras

A más frecuencia del fraude para las instituciones financieras, mayor será el desafío para atacarlo. Los factores que contribuyen a este desafío son: el gran volumen de transacciones manejadas por la mayoría de las instituciones frente al número relativamente pequeño de transacciones fraudulentas, la velocidad con la que la tecnología permite que los defraudadores operen, datos incompletos y la falta de intercambio de información entre las instituciones financieras. Con demasiada frecuencia, los bancos carecen de la tecnología y las capacidades para implementar las salvaguardias necesarias, respondiendo a un problema principalmente digital de una manera analógica -por ejemplo, llamadas telefónicas que intentan reconstruir el camino de una serie de transferencias inusuales de dinero.

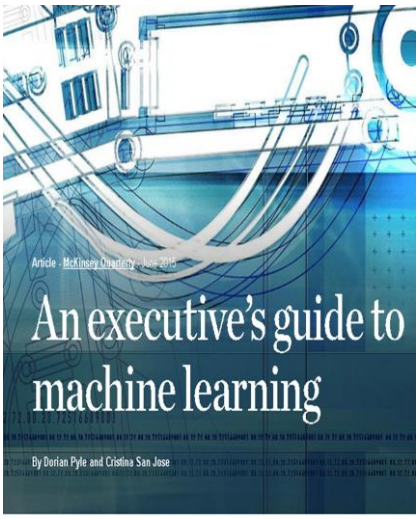
Al combinar conjuntos de datos propietarios con puntos de referencia de la industria e información gubernamental, las instituciones financieras pueden utilizar inteligencia artificial, aprendizaje automático y análisis en la lucha contra el fraude financiero. Este artículo de McKinsey nos muestra un caso aplicado del uso de aprendizaje automático - "machine learning" - exitoso realizado en un banco por la empresa QuantumBlack mediante el análisis de pago de facturas fraudulentas.

http://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/applying-analytics-in-financial-institutions-fight-against-fraud?cid=other-eml-alt-mip-mck-oth-1704

Una Guía Ejecuiva sobre el "Aprendizaje Automático" o "Machine Learning"

En el artículo anterior mencionamos un ejemplo de "machine learning" para detectar fraude en el pago de facturas de un banco. Por esta razón pensamos que sería una buena idea introducir un documento, también de la consultora McKinsey de hace año y medio, para que nos ayude a descubrir, definir y sobre todo a utilizar el lenguaje especial del "machine learning" para aquéllos que no somos especialistas.

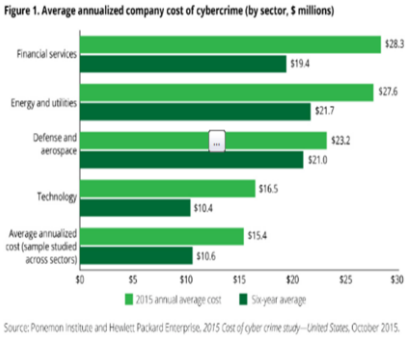
El aprendizaje automático se basa en algoritmos que pueden aprender de datos sin depender de la programación basada en reglas predeterminadas. Entró como una disciplina científica a finales de 1990 gracias a los avances constantes en la digitalización y la reducción en el costo de las computadoras, permitió a los científicos de datos dejar de construir modelos cerrados y en su lugar de ello, dejar que las computadoras lo hagan.



http://www.mckinsey.com/industries/high-tech/our-insights/an-executives-guide-to-machine-learning

Las empresas financieras confrontan la ciberseguridad

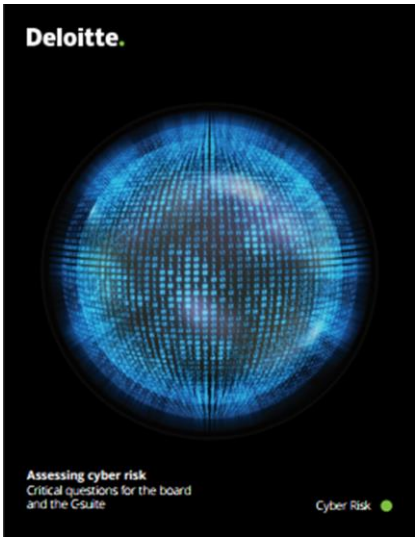
El Centro de Servicios Financieros de Deloitte entrevistó a los principales oficiales de seguridad de la información (CISO por sus siglas en inglés) ya expertos en administración de riesgos cibernéticos de los sectores de banca, seguros y administración de inversiones para identificar los mayores desafíos que enfrentan. Los entrevistados compartieron historias de guerra cibernética, citando una amplia variedad de obstáculos y frustraciones. Algunos encuestados se describen a sí mismos como "la primera línea de respuesta", poniendo una serie interminable de "incendios forestales" al tratar de interceptar un "ciber infierno" que podría acabar con la empresa.



http://deloitte.wsj.com/riskandcompliance/2017/03/24/financial-firms-confront-cyber-risk/

Evaluando el riesgo de ciberseguridad: Preguntas críticas al Directorio y la Alta Gerencia

En casi la totalidad de nuestros países, los entes directivos, reguladores, gestores de riesgo y como no, nosotros los auditores, venimos investigando y analizando las mejores prácticas para evaluar el riesgo de ciberseguridad. Incluso hay ya varios macros integrales –el propio del IIA Global, NIST, FFIEC, entre otros- y hace poco el Gobierno federal de Nueva York publicó el suyo.
Mientras tanto, compartimos este interesante documento guía de Deloitte que nos comenta las 10 preguntas que nuestros directivos "deben" contestar:
1. ¿Demostramos la debida diligencia, la propiedad y la gestión eficaz del riesgo cibernético? 2. ¿Tenemos el liderazgo correcto y el talento organizativo? 3. ¿Hemos establecido un marco apropiado de escalamiento del riesgo cibernético que incluya nuestro apetito de riesgo y los umbrales de reporte? 4. ¿Estamos enfocados e invertimos en lo correcto? 5. ¿Cómo se alinean nuestros programas y capacidades de riesgo cibernético con los estándares de la industria y las organizaciones similares? 6. ¿Tenemos una mentalidad cibernética y una organización de cultura cibernética? 7. ¿Qué hemos hecho para proteger a la organización contra riesgos cibernéticos de terceros? 8. ¿Podemos contener rápidamente daños y movilizar recursos de respuesta cuando ocurre un incidente cibernético? 9. ¿Cómo evaluamos la efectividad del programa de riesgo cibernético de nuestra organización?, 10. ¿Somos un link seguro en los ecosistemas altamente conectados en los que operamos?



https://www2.deloitte.com/global/en/pages/risk/articles/assessing-cyber-risk.html?id=us:2em:3na:cyberrisk:awa:adv:042017#

Administrando el Riesgo desde la Primera Línea

En esta encuesta global hecha a casi 1,600 gerentes corporativos de 80 países, PwC evalúa la evolución de la gestión de riesgos en su sexta edición.
Casi el 63% de los encuestados respondió que trasladar la responsabilidad por los riesgos a la primera línea de defensa hacía a las empresas más ágiles –es decir mejor posicionadas para anticipar y mitigar eventos de riesgo- y el 46% planeaba amplificar este cambio en los próximos 3 años.

pwc

http://www.pwc.com/riskinreview