BHR MÉXICO
Contadores Públicos Certificados, Abogados y Consultores

SFAI GLOBAL

Abril **2026**

Área: Auditoría

Inteligencia artificial y fraude: el nuevo nivel de exposición corporativa

Resumen: La auditoría se convierte en una herramienta estratégica para la Dirección General al asegurar información confiable y oportuna, permitiendo anticipar riesgos, mejorar el control y tomar decisiones con mayor certeza.

Escrito por:
José Luis Zamora Morales - Socio

dn@bhrmx.com
www.bhrmx.com

El fraude digital dejó de ser un conjunto de eventos aislados, para convertirse en un sistema estructurado, escalable y altamente eficiente. Hoy opera bajo una lógica distinta: combina automatización, inteligencia artificial y activos virtuales para ejecutar ataques más precisos, rápidos y difíciles de rastrear.

El cambio no es solo tecnológico, es operativo. Los esquemas actuales no dependen del volumen, sino de la calidad del ataque. Esto significa menos intentos, pero con mayor probabilidad de éxito y con impactos económicos significativamente más altos. En este entorno, los mecanismos tradicionales de control —diseñados para errores humanos o fraudes básicos— ya no responden al nivel de sofisticación actual.

Puntos críticos para la Alta Dirección

El riesgo se ha desplazado hacia procesos clave del negocio. Los ataques se concentran en puntos donde existe flujo de dinero, toma de decisiones o acceso a información sensible. Tesorería, pagos a proveedores, autorizaciones ejecutivas y canales digitales se han convertido en los principales vectores de entrada.

La inteligencia artificial está jugando un papel determinante. Hoy permite replicar patrones de comunicación, generar mensajes altamente creíbles e incluso simular identidades con un nivel de precisión que supera los controles convencionales. Esto elimina una de las principales barreras históricas del fraude: la detección por sentido común.

Adicionalmente, los esquemas actuales son acumulativos. Un mismo ataque puede combinar suplantación de identidad, manipulación psicológica y ejecución financiera en cuestión de horas, reduciendo al mínimo la ventana de reacción.

Impacto financiero para la Alta Dirección de las entidades o C-Level

El impacto ya no está en la frecuencia, sino en la magnitud. Los fraudes actuales están diseñados para capturar montos relevantes en una sola operación, afectando directamente la liquidez y, en casos extremos, la continuidad del negocio.

Los activos virtuales, particularmente las criptomonedas, han acelerado este fenómeno. Su uso permite mover recursos de forma inmediata, sin intermediarios y con alta complejidad de rastreo, lo que dificulta la recuperación de fondos. Esto ha convertido a las transferencias digitales en uno de los puntos más vulnerables dentro de la operación financiera.

Al mismo tiempo, los esquemas de suplantación corporativa han evolucionado. Ya no se limitan a correos falsos, sino que integran múltiples canales y momentos de interacción, generando confianza antes de ejecutar la instrucción financiera. Esto incrementa la probabilidad de que los controles internos sean superados sin generar alertas inmediatas.

Implicaciones de control y cumplimiento

El entorno actual exige una redefinición de los controles internos. La segregación de funciones, las validaciones manuales y los procesos de autorización lineales ya no son suficientes frente a esquemas que operan en tiempo real y con alto grado de personalización.

Se vuelve indispensable incorporar niveles adicionales de control, como validaciones independientes, monitoreo transaccional continuo, análisis de comportamiento y mecanismos robustos de autenticación. Asimismo, la trazabilidad de operaciones y la capacidad de respuesta ante incidentes deben formar parte del diseño operativo, no como reacción, sino como prevención.

Otro punto crítico es la integración entre áreas. El fraude digital ya no es un tema exclusivo de tecnología o cumplimiento; involucra diversas áreas como son: finanzas, operaciones, legal y dirección general. La falta de alineación entre estas funciones incrementa significativamente la exposición.

Señales de riesgo en el entorno actual

Se observan patrones cada vez más claros en la evolución del fraude. Los ataques están dirigidos a estructuras organizacionales complejas, donde la velocidad de operación y la confianza interna juegan en contra del control. También se identifican esquemas que aprovechan eventos externos, tendencias tecnológicas o contextos regulatorios para generar credibilidad.

Destaca la combinación de tecnologías emergentes con tácticas tradicionales. La inteligencia artificial se utiliza para construir el engaño, mientras que los activos digitales permiten concretar la extracción de recursos. Este modelo híbrido representa el estándar actual del fraude.

José Luis Zamora
Socio

En conclusión, el fraude digital ya no es un riesgo operativo menor, sino un riesgo estratégico que impacta directamente la estabilidad financiera y la toma de decisiones. La velocidad con la que evolucionan los esquemas supera la capacidad de adaptación de muchas organizaciones, generando una brecha crítica entre riesgo y control.

La verdadera exposición no está en la ausencia de controles, sino en la falsa sensación de seguridad que generan estructuras que ya no responden al entorno actual.

En BHR México apoyamos a las organizaciones en la identificación y mitigación de riesgos asociados al fraude digital, mediante evaluaciones de control interno, análisis forense, cumplimiento en PLD y fortalecimiento de procesos críticos como tesorería, y automatizar procesos financieros-fiscales, para tener mayor control, visibilidad en tiempo real y mucha más certeza sobre los datos que usas para decidir así como en aplicar evaluaciones de confianza con herramientas tecnológicas utilizando la inteligencia artificial.

Si tu organización mantiene operaciones digitales o realiza transferencias relevantes, es momento de evaluar si los controles actuales realmente resisten un entorno donde el fraude ya opera con inteligencia artificial y estructuras financieras descentralizadas.

José Luis Zamora
Socio