La Ciberseguridad, inteligencia artificial y confianza pública: la nueva Frontera del control interno en Administración y Finanzas

Introducción

La digitalización ha trasladado una parte sustancial de la gestión financiera a sistemas, plataformas y flujos automatizados. Hoy, una orden de pago puede recorrer varias aplicaciones antes de llegar al banco, un cambio en el maestro de proveedores puede modificar el destino de una transferencia y una herramienta de inteligencia artificial puede intervenir en tareas que antes dependían enteramente del juicio humano. Esa realidad ha acercado la ciberseguridad al núcleo de Administración y Finanzas.

Pagos, registros contables, facturación, conciliaciones, nóminas, declaraciones tributarias y reportes dependen de información digital. Cuando esa información pierde integridad, confidencialidad o disponibilidad, el problema deja de ser estrictamente tecnológico. El efecto alcanza la liquidez, el cumplimiento, la prevención del fraude, la continuidad de las operaciones y la credibilidad de los estados financieros.

Desde esta perspectiva, la ciberseguridad forma parte de la arquitectura de control interno. No implica trasladar al contador las funciones propias de Tecnología. Exige reconocer una interdependencia: Tecnología resguarda el entorno técnico, mientras Administración y Finanzas conocen la sustancia de las operaciones, identifican los procesos críticos y determinan cuándo una transacción es razonable, autorizada y debidamente sustentada.

1. Cuando el riesgo tecnológico Impacta el corazón de las finanzas

Una vulneración no siempre comienza con un evento visible. A veces surge de una credencial compartida, un acceso que nunca fue revocado, una cuenta de servicio con privilegios excesivos o una modificación aparentemente rutinaria en los datos bancarios de un proveedor. El riesgo se materializa cuando esa debilidad permite registrar, aprobar, modificar o ejecutar una operación sin la debida legitimidad.

Para confiar en una cifra no basta con verificar su exactitud aritmética. También importa conocer su procedencia, quién la registró, quién la aprobó, qué modificaciones sufrió y qué evidencia respalda la transacción. La trazabilidad aporta esa memoria institucional. Permite reconstruir el recorrido de una operación y distinguir un error operativo de una alteración deliberada.

Ejemplos de Vulnerabilidades con impacto financiero

- **Datos maestros de proveedores:** un cambio no autorizado en la cuenta bancaria de un suplidor puede desviar pagos legítimos hacia un tercero y pasar inadvertido si el proceso carece de validaciones independientes.
- **Sistemas de nómina:** la modificación de empleados, salarios o cuentas bancarias puede originar desembolsos indebidos y afectar información laboral sensible.
- **Facturación electrónica:** una alteración en interfaces, secuencias o datos fiscales puede generar inconsistencias, rechazos, sanciones y diferencias entre la contabilidad y la información reportada a la administración tributaria.
- **Plataformas de tesorería:** una interrupción, una credencial comprometida o una instrucción manipulada puede afectar pagos, disponibilidad de efectivo y cumplimiento de obligaciones inmediatas.

Ataques de ransomware, apropiación de credenciales y fraude interno muestran una misma lección. Recuperar un sistema es apenas una parte de la respuesta. La organización también necesita preservar evidencia, revisar accesos, identificar la causa, evaluar las operaciones ejecutadas durante el incidente y corregir las salvaguardas afectadas. Sin esa revisión, el servicio puede restablecerse mientras la vulnerabilidad permanece.

2. Inteligencia artificial e identidades digitales: nuevos actores dentro del control

La inteligencia artificial amplía la capacidad de automatizar análisis, clasificaciones, conciliaciones y tareas administrativas. Su incorporación aporta eficiencia, pero introduce interrogantes que el control interno debe atender con criterio. La velocidad de una herramienta no sustituye la rendición de cuentas, y una recomendación automatizada no elimina la necesidad de validación cuando existe impacto financiero.

- **Uso de datos:** debe definirse qué información puede procesar una herramienta de IA, dónde se almacena y bajo qué condiciones puede ser compartida.
- **Acciones automatizadas:** cuando una solución genera, modifica o propone transacciones, la organización debe establecer límites, niveles de aprobación y evidencia de la intervención realizada.
- **Identidades no humanas:** cuentas de servicio, bots, integraciones y agentes digitales requieren responsable, vigencia, permisos delimitados y revisión periódica, al igual que cualquier usuario con acceso sensible.
- **Continuidad operativa:** los planes de recuperación deben contemplar los procesos financieros esenciales, sus dependencias tecnológicas y las alternativas de operación cuando una plataforma no esté disponible.
- **Digitalización tributaria:** la creciente conexión entre facturación, libros contables y plataformas fiscales exige proteger la integridad de los datos desde su origen hasta su presentación ante las autoridades.

3. Responsabilidades de Tecnología y Administración y Finanzas

El Departamento de Tecnología asume la custodia técnica del entorno digital. Le corresponde administrar la infraestructura, la seguridad de redes y sistemas, la gestión de identidades y accesos, el monitoreo de amenazas, la atención de vulnerabilidades, los respaldos, la recuperación ante incidentes y las condiciones de seguridad aplicables a herramientas de inteligencia artificial. También debe conservar registros técnicos suficientes para investigar eventos y demostrar qué ocurrió cuando se presenta una anomalía.

Esa responsabilidad no desplaza la de Administración y Finanzas. Tecnología puede proteger una plataforma, pero necesita que el negocio identifique cuáles operaciones son sensibles, qué accesos resultan incompatibles, qué cambios requieren doble validación y qué información debe recuperarse primero ante una interrupción. La eficacia del control depende de esa coordinación. Cuando cada área conoce su ámbito y comparte evidencia, se reduce la posibilidad de vacíos, duplicidades y responsabilidades difusas.

En la práctica, esta articulación debe traducirse en controles verificables:

- **Segregación de funciones:** evitar que una misma persona pueda crear o modificar un proveedor, registrar la factura y ejecutar el pago sin una revisión independiente.
- **Gobernanza de accesos:** asignar permisos según las funciones reales, revisar privilegios sensibles y retirar oportunamente accesos innecesarios.
- **Trazabilidad:** conservar evidencia de altas, modificaciones, aprobaciones, interfaces, ejecuciones y excepciones relevantes.
- **Continuidad:** definir prioridades de recuperación, responsables, procedimientos alternos y criterios para validar la integridad de la información una vez restablecidos los sistemas.
- **Gobernanza de IA:** establecer reglas sobre datos, autorizaciones, supervisión humana, registro de acciones y responsabilidades cuando una herramienta automatizada intervenga en procesos financieros.
- **Coordinación interdisciplinaria:** mantener una relación operativa entre Tecnología, Finanzas, Auditoría y Cumplimiento para conectar el riesgo técnico con sus consecuencias económicas y regulatorias.

4. El rol del profesional contable

No se espera que el profesional contable configure un firewall, investigue código malicioso o administre una plataforma de detección de amenazas. Su contribución nace del conocimiento del proceso y de su capacidad para reconocer cuándo una operación rompe la lógica del negocio. Ese conocimiento resulta especialmente valioso porque muchas irregularidades tecnológicas terminan expresándose como una transacción financiera.

Preguntas sencillas suelen exponer debilidades relevantes: ¿quién puede modificar los datos bancarios de un proveedor?, ¿quién aprueba ese cambio?, ¿el sistema conserva evidencia?, ¿existen usuarios con funciones incompatibles?, ¿una cuenta automatizada conserva privilegios superiores a los necesarios?, ¿la organización puede recuperar la información requerida para pagar, conciliar y reportar?

El profesional contable aporta discernimiento sobre materialidad, razonabilidad, evidencia y rendición de cuentas. Esa mirada complementa la especialización técnica y evita que la ciberseguridad se reduzca a una discusión de herramientas. El objetivo final es proteger la calidad de la información sobre la cual se toman decisiones y se responden obligaciones frente a terceros.

5. Confianza pública: más allá de una cifra correcta

Accionistas, entidades financieras, reguladores, clientes, proveedores y auditores toman decisiones a partir de información preparada, procesada o revisada por las áreas financieras. Una cifra puede ser matemáticamente correcta y, aun así, provenir de un proceso vulnerable. Por eso la confianza no descansa únicamente en el resultado, también depende de la solidez del recorrido que produjo ese resultado.

La confianza pública se fortalece cuando la organización puede demostrar quién hizo qué, con qué autorización, en qué momento y con qué evidencia. Esa capacidad cobra mayor relevancia en procesos automatizados, donde parte de la ejecución puede recaer en interfaces, robots o agentes digitales. La automatización cambia al ejecutor, pero no extingue la responsabilidad institucional.

Los comités de auditoría y las áreas de Finanzas tienen aquí una responsabilidad de supervisión. Incorporar los riesgos digitales a sus revisiones periódicas, conocer las dependencias tecnológicas de los procesos críticos y exigir planes de respuesta contribuye a una gestión más prudente. La ciberseguridad deja entonces de percibirse como un asunto aislado de sistemas y pasa a formar parte de la conversación sobre control, continuidad y buen gobierno.

Conclusión

La ciberseguridad y la inteligencia artificial han ensanchado el perímetro del control interno. Hoy, proteger la información financiera implica custodiar accesos, identidades digitales, interfaces, evidencias y decisiones automatizadas con el mismo rigor aplicado tradicionalmente a autorizaciones, conciliaciones y segregación de funciones.

La responsabilidad debe permanecer claramente distribuida. Tecnología responde por la protección técnica, el monitoreo, la resiliencia y la recuperación de los sistemas. Administración y Finanzas identifican la criticidad de los procesos, validan la legitimidad de las operaciones y definen los controles de negocio. Auditoría y Cumplimiento aportan evaluación independiente y vigilancia sobre el diseño y funcionamiento de esas salvaguardas. Ninguna de estas miradas resulta suficiente de manera aislada.

En definitiva, la confianza pública se preserva cuando una organización puede sostener sus cifras con procesos íntegros, evidencia verificable y responsabilidades inequívocas. La tecnología modifica la forma de trabajar y la inteligencia artificial incorpora nuevos participantes digitales, pero el deber de responder por la información financiera continúa siendo humano. Esa responsabilidad compartida constituye una expresión concreta de ética profesional, prudencia y buen gobierno.

Referencias

KPMG International. (2026). Cybersecurity considerations 2026: Eight key cybersecurity considerations for 2026.

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology.

Tabassi, E. (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2019). Managing Cyber Risk in a Digital Age.

Altagracia Maribel Mateo Chalas
Contadora Pública Autorizada
Magíster en Contabilidad Tributaria
Auditora Forense Antifraude (AFA)
Miembro de la Comisión de Administración y Finanzas de la AIC
Correo: altagraciamateo01@gmail.com