CAPÍTULO 3

Desafíos en ciberseguridad

3.1. Desafíos y riesgos de la IA en la contabilidad

Los temas hasta el momento, han mostrado una sutil manera de entrelazarse dado que la naturaleza del abordaje de la IA implica varias cosas a la vez cuando se trata de su explicación y análisis. Eso significa que abundaremos en algunos puntos que ya se han venido tratando dado que los riesgos vienen en muchas ocasiones, de la mano de las ventajas, donde la IA representa todo un campo de estudio que ha venido en constante crecimiento durante los últimos años yendo más allá de lo hipotético y aterrizando en realidades aplicadas que generan la experiencia necesaria entre organizaciones y particulares para generar investigación fiable acerca de su uso. La identificación de los riesgos y su gestión, forman también, parte de la preocupación del profesional contable e incluso, parte de su formación académica necesaria para entrar de cara al futuro del uso de las IAs en la contabilidad, convirtiendo esos riesgos en oportunidades de repensar, establecer nuevas formas de abordaje e incluso colaborar con las muy necesarias normativas al respecto, que al final, se convierten en parte de los propósitos de este libro.

3.2. Sesgos algorítmicos y la falta de explicabilidad (el fenómeno "*black box*")

El sesgo algorítmico es uno de los problemas más citados en términos del *machine learning*, donde uno podría esperar que sea el proceso más "limpio" del trabajo con las IAs.

Este tipo de preocupaciones se remite a la falta de neutralidad en la programación de la IA comúnmente utilizada, sea intencional o por descuido, lo que puede arrojar datos equivocados para su interpretación. Pero, ¿por qué hablar de una *black box*? Recordemos que se le da este nombre a una grabadora de vuelo de avión, un dispositivo resistente al daño para poder investigar los accidentes o siniestros en un vuelo y metafóricamente se refiere a sistemas cuyo funcionamiento es desconocido y del que sólo obtenemos información de entrada y salida. En el contexto de la IA esto resulta ser algo adecuado, ya que los modelos avanzados como el *machine learning* y el *deep learning* funcionan así.

Un ejemplo de *black box* en contabilidad, sería el siguiente:

Input o datos de entrada: Al sistema se le entregan datos de registros financieros.

Procesamiento interno: Los algoritmos trabajan haciendo cálculos complejos, usando millones de parámetros con los que fueron programados y correlaciones estadísticas.

***Output* o salida:** El modelo entrega sus resultados de, por ejemplo, predicciones de riesgos de inversión.

Siguiendo la descripción acerca del funcionamiento de la *black box*, lo que ocurre es que la fase de procesamiento interno no es comprensible ni transparente para los involucrados. La cuestión radica en que, si el usuario final hace una pregunta acerca del proceso, como sería, basándonos en el ejemplo de arriba, querer saber si los porcentajes de predicción se ajustan al caso del registro, eso es algo que el sistema no puede explicar lo cual complica el trabajo del contador porque no tiene claridad para trazar la información y justificar o responder a las dudas de algún intere-

sado. Esto genera un gran problema porque esa falta de claridad puede obedecer a varias cosas: desde información mal sometida como datos de entrada, hasta un sobreajuste (*overfitting*) a datos previos que no responde al caso que se está observando. Esto genera riesgos muy serios, no sólo por la falta de explicabilidad como ejemplificamos, también puede afectar a la reputación de la organización contable que respalde este tipo de análisis y el riesgo de incumplimiento con principios de transparencia y objetividad. Esto también provoca una falta de regulación en los procesos de rendimiento de informes por parte del profesional contable. Sencillamente la fiabilidad del trabajo con la IA queda en entredicho.

El problema con los sesgos algorítmicos es que son una (si no es que la más grande) contra que tienen estos sistemas en la actualidad. La promesa del *machine learning* en términos de traer mayor disciplina a los procesos de toma de decisiones y volver relevante su uso en el futuro, cae mucho gracias a este tipo de problema. Es usualmente conocido que herramientas como *ChatGPT* no son del todo fiables y aun así se siguen construyendo y realizando estudios, investigaciones, trabajos académicos y hasta de investigación formal con esa herramienta de apoyo, delegando en ella el peso casi total del trabajo (veremos más de eso en el siguiente apartado). Eso significa un gran golpe para la fidelidad al conocimiento y la verdad, sea en un extremo ético o uno de confianza profesional. Barrocas, Hardt y Narayan (2019) plantean un interesante debate al respecto de este desafío, donde identifican tres niveles de discriminación que pueden generar problemas de programación de algoritmos de una IA y generan sesgos en sus productos.

3.3. Los tres niveles de discriminación y su repercusión en el uso de las IAs contables

Según sociólogos, existen tres tipos de discriminación que son estructurales, organizacionales e interpersonales, siendo la primera por la manera en que se organiza la sociedad, que se puede interpretar por leyes discriminatorias y otras más suaves como normas y costumbres, como actitudes clasistas. Los factores organizacionales operan a nivel de organizaciones o unidades de toma de decisiones como las compañías que contratan empleados. Los factores interpersonales se refieren a actitudes y creencias que resultan en conductas discriminatorias de los individuos. La discriminación también puede ser directa o indirecta, siendo la primera aquella que toma acciones o procesos de decisiones haciendo referencia sobre atributos específicos y la indirecta que toma acciones o procesos de decisiones no haciendo referencia explícita, pero que genera desventaja sobre uno o más grupos (Barocas, Hardt y Narayan, 2019, p.209).

En términos del mundo digital, se encuentran varios ejemplos de estas características que pueden tener amplitud de detección. Pensemos en el sonado tema de las *cookies* que se regularizó no hace mucho, el cual no explicaba a los usuarios que navegan en internet la información que las páginas visitadas tomaban de ellos y los terceros a quienes eran entregados. Esto puede llevar a muchas cosas, desde fraude y suplantación de identidad, hasta tipos de segmentación de los mercados y calificación para créditos y sus tipos. Esta opacidad, como explica Burrell (2016), impide conocer el proceso que ocurre entre la entrada (*input*) de los datos que obtienen y el resultado (*output*) que por lo general son clasificaciones de usuarios o potenciales clientes de infinidad de destinos aparte de los ya mencionados

para instituciones bancarias o crediticias. Además, hay que tomar en cuenta que la información de *input* debería ser entregada voluntariamente o al menos ser reconocida por los usuarios. La opacidad no sólo radica en el desconocimiento del proceso (el qué se hace con la información) sino también con los propietarios de la información, lo cual conlleva efectos evidentemente discriminatorios. La opacidad incurre, nos dice Burrell, en tres formas:

> a) opacidad como autoprotección y ocultamiento intencional corporativo o institucional y, junto con ella, la posibilidad de engaño consciente; b) la opacidad que surge del estado actual de cosas donde escribir (y leer) código es una habilidad especializada y; c) una opacidad que surge del desajuste entre la optimización matemática en alta dimensionalidad característica del aprendizaje automático y las demandas del razonamiento a escala humana y los estilo de interpretación semántica (Burrell, 2016).

Al final, estar conscientes de que esto ocurre, ayuda a tomar en cuenta los errores en los que el profesional de la contabilidad no debe caer y contribuir a que las organizaciones donde trabaja y en las que se involucra en términos de rendimiento de cuentas, tampoco lo hagan. Frank Pasquale (2015) ya advertía acerca de que, aunque la automatización de los procesos supone una regulación de los sesgos y decisiones apresuradas en el ámbito financiero, los marcos en los que se desenvuelve el fenómeno de la caja negra, sólo se han unido a esa automatización, pues diversas crisis se han podido observar ya que las finanzas cibernéticas también son capaces de generar ventajas injustas que terminan por beneficiar a organizaciones mejor posicionadas. Es entonces que los algoritmos se pueden oscurecer por una triple capa de complejidad técnica, se-

crecía y “espionaje económico” que no nos permite saber qué es lo que ocurre en los niveles financieros mayores. Si la IA está a cargo de esas firmas, es decir, intereses mayores, es posible que el fenómeno de la inexplicabilidad acreciente su estadía como un desafío a seguir enfrentando en los años por venir.

3.4. Dependencia excesiva y pérdida de pensamiento crítico en la contabilidad con IA

Se puede decir que todos los caminos de los desafíos llevan a este sitio. En primera instancia porque entendemos que el fenómeno de la IA maximiza la idea de que el trabajo humano represente el menor esfuerzo y este pueda ser delegado para tareas más complejas o incluso, sencillas. O al menos esa parece ser la actitud reinante en los planteamientos más comunes del por qué es de utilidad el uso de estas tecnologías. Dentro de la contabilidad como en cualquier área, se puede generar una dependencia excesiva de esta herramienta, sobre todo por lo encantadora que puede lucir y, como ya hemos estado viendo en este capítulo, eso puede ser engañoso.

La automatización del trabajo puede llevar a ciertos sesgos cognitivos, fosos que hacen que el juicio tome ciertos atajos acerca de lo que la IA parece representar. Carr (2014) le llama el efecto degenerativo, donde la gente comienza a caer en ciertos aspectos dañinos para el pensamiento crítico. Sesgos como la complacencia que lleva a un falso sentido de seguridad y provoca la falta de compromiso, dejando el encargo a la máquina, ignorando información que pueda provenir de otras fuentes y que presente un conflicto con los resultados de la IA. El impacto que esto puede causar al proceso de aprendizaje y la pericia en los campos de estudio puede ser incalculable a causa de este sesgo y otros

tantos que pueden surgir. No es extraño cuando pensamos en la dificultad que las nuevas generaciones tienen para la retención y comprensión cuando dicha tarea se delega a una IA o al exceso informativo que hace engorroso elegir (que también tiene sus propios sesgos) donde la carga cognitiva trata de que se requiere cierto nivel de dificultad para poder pensar a fondo (Blashki, 2025). Será entonces que el pensamiento crítico comienza a perder su impacto en nuestras habilidades al dejar de discernir y profundizar en la información que manejamos, con tal de ocuparse en otras tareas. Incluso amenazando las habilidades naturales de aprendizaje del ser humano.

Así que, si llevamos esto al terreno contable, podemos identificar cuatro riesgos presentes en esta excesiva confianza en la tecnología algorítmica:

Aceptar resultados de forma acrítica: Se puede llegar a validar de forma errónea la información que algún modelo contable automatizado llegue a entregar, sea de manera incorrecta o no, el profesional contable puede "brincarse" la duda o el proceso de inquirir sobre los resultados.

Competencias humanas erosionadas: Habilidades básicas del contador como el análisis, interpretación y juicio ético, pueden perderse y dejar de ser fundamentales en su ejercicio al delegar responsabilidades a la IA.

Dificultad para detectar errores: El asunto con los modelos de IA avanzados, es que son buenos sistemas de trabajo con patrones grandes, es decir, trabajan mejor con la generalidad que con el aspecto más sutil. Puede haber inconsistencias contextuales que el contador pueda ubicar gracias a su experiencia y pensamiento crítico. Anteriormente tocamos el tema sobre el detalle, el llamado "ojo clínico" para poder detectar inconsistencias gracias al análisis profundo.

Un rol estratégico debilitado o inexistente: Se debe decir claramente que el profesional contable que depende demasiado de la IA termina por convertirse en un operador de esta, en lugar de ser un profesional capacitado y equipado con juicio crítico y estratégico.

Volviendo a Carr, los avances tecnológicos no son "malos" per se, ni tampoco tienen por qué llegar a serlo (2014). La automatización, en todo caso, debería ser capaz de ayudarnos a apuntalar nuestro pensamiento crítico, altamente relacionado a nuestra creatividad que al final, es un pensamiento que genera alternativas. Deberían, en todo caso, habilitar ese pensamiento, procurando cuidado, fomentando la duda y una cultura del cuestionamiento. La tarea precisamente, es evitar que el trabajo con algoritmos desplace la interpretación humana (Floridi, 2014), ya que esto significaría un problema en el encargo profesional, desde el cual, también ha de fomentarse la formación continua, siendo todo esto una especie de red apoyo que obligue a que la automatización no sea acrítica, sino todo lo contrario. El pensamiento crítico habrá de prevalecer siempre y cuando consideremos a la IA como una herramienta y no como un sillón de descanso.

3.5. Privacidad de datos y ciberseguridad

Uno de los retos más grandes que afronta la inteligencia artificial en el tema financiero, es el de la gestión de los datos sensibles (patrimoniales, financieros, fiscales y personales, entre otros). El tema de la protección, privacidad y seguridad, es uno de los que más han llamado la atención cuando se habla en el uso de tecnologías algorítmicas y no es para menos. Tan sólo en 2024, el ciberfraude (que incluye hackeo, *deepfake*, clonación de voz y *phishing* altamente sofisticado) fue causa de ataques al 90% de empresas

estadounidenses y las pérdidas en casi la mitad de ellas ascienden a más de 10 millones de dólares (Trustpair, 2025), lo cual ya habla de la gravedad del asunto. Bischoff (2023) reportó que, entre 2018 y 2023, 2260 brechas de datos en el sector financiero, lo cual significa que la explotación de datos, los cuales incluyen datos bancarios, números de seguridad social, contraseñas y números de identificación de impuestos, afectaron 232 millones de registros. El también llamado crimen digital está arrojando números que pueden llegar a lo dramático y demuestra la vulnerabilidad del sector financiero y contable como auténticos temas de preocupación en diversos sectores.

La estimación que informa el *IBM Cost of a Data Breach Report* 2024, es que el costo promedio de una brecha de datos a nivel mundial está alcanzando los 4.96 millones de dólares en este 2025, mientras que los costos pueden llegar a 375 millones de dólares en brechas masivas (IBM, 2024). Un dato importante que señala este informe es que el tiempo promedio para detectar una brecha en este sector es de 168 días, lo cual implica que los daños pueden extenderse durante meses de forma silenciosa, antes de ser detectados y, por consiguiente, contenidos.

Una de las tareas principales y riesgos mayores en el trabajo financiero en la actualidad, es el manejo de datos sensibles en entornos cibernéticos, lo cual implica una exposición debido al entorno digital en el que estos se suelen hallar. La sistematización de los datos en dicho entorno, tiene la contra declarada de un valor altísimo para crímenes digitales que hacen que urjan regulaciones y protección en términos de seguridad y gobernanza ética.

3.6. Privacidad de datos financieros

La privacidad de los datos de los individuos es un derecho y las instituciones y organizaciones que tienen control de sus datos están obligadas a protegerlos y no tenerlos expuestos para engrosar la economía de terceros (sobre todo porque la falta de regulaciones hace que esos datos puedan formar parte del catálogo de organizaciones con las que no existe convenio por parte de los particulares), que, ya se ha visto, pueden ser utilizados con diversos fines, incluso prestarse para fraudes. El *World Economic Forum* (2024) en su encuesta de percepción de riesgos globales 2023-2024, en la que se consulta a 1500 expertos alrededor del mundo, sobre los riesgos mundiales que afrontaremos, toca a la ciber inseguridad en el cuarto lugar de las preocupaciones de dichos expertos previstas para dos años (lo que sería 2026) y a 10 años ubican en sexto lugar a los resultados adversos en el uso de tecnologías IA, solamente superada por temas relativos al cambio climático. Aun así, ambas preocupaciones, encabezan las problemáticas que los expertos observan y que están relacionadas al entorno digital.

Los riesgos pueden estar más claros si vamos más allá de lo técnico. Esto es, tan sólo pensemos en la información que se encuentra en la nube: nuestro drive de Google donde se guardan documentos personales, a veces notas, facturas y otros documentos que pueden contener datos fiscales y que, incluso muchas organizaciones utilizan para respaldar información sensible. Pensemos en las plataformas de big data (término utilizado para describir grandes almacenamientos de datos, comprendidos en volumen y variedad) con toda la información que transita en la web y que puede llegar a ser fácilmente monitoreada.

3.7. Seguridad cibernética o ciberseguridad

La ciberseguridad es una disciplina basada en computación, compleja que integra gente, información y procesos para proteger sistemas de accesos no autorizados o ataques (Joint Task Force in Cyberscurity, 2018 en Kovacevik y cols., 2025). El hecho de que exista la ciberseguridad es debido al tipo de ataques que ya hemos venido comentando, pero en justa medida con el nivel de desarrollo de la IA, los tipos de ataque también se han complejizado. Veamos algunos de los más comunes relacionados al mundo financiero y contable, en la siguiente tabla:

Tabla 2

Principales ciberataques asociados al ámbito financiero y contable.

Tipo de ataque	Definición general	Mecanismo o medio de ataque	Finalidad o impacto	Relevancia en el ámbito contable-financiero	Referencia
Phishing	Envío de correos o mensajes fraudulentos que imitan fuentes legítimas.	Se usa correo electrónico, SMS o mensajes instantáneos para inducir al usuario a entregar credenciales o datos financieros.	Robo de contraseñas, claves bancarias y datos de acceso a sistemas contables.	Afecta directamente la seguridad de los sistemas financieros, permitiendo accesos indebidos a cuentas, plataformas o registros contables.	Kovacevik, 2025; Kaspersky, 2025
Deepfakes financieros	Suplantación de identidad mediante IA generativa (voz, imagen o video).	Algoritmos de IA recrean la voz o apariencia de personas (directivos, socios o auditores).	Falsificación de documentos, autorizaciones o comunicaciones internas.	Riesgo en validaciones de operaciones, aprobaciones falsas y manipulación de auditorías.	Kovacevik, 2025

Malware	Software malicioso diseñado para infiltrarse, dañar o robar información.	Se instala por medio de archivos adjuntos, descargas o enlaces maliciosos.	Robo, alteración o destrucción de datos contables y financieros.	Compromete la integridad de la información contable; puede alterar balances o destruir respaldos.	Kaspersky, 2025
Ransomware	Variante de malware que secuestra datos cifrándolos para exigir rescate.	Infecta sistemas y bloquea el acceso a los datos del usuario.	Extorsión económica a cambio de recuperar la información cifrada.	Riesgo severo en firmas contables por pérdida temporal o definitiva de bases de datos críticas.	Kaspersky, 2025
Ingeniería social	Manipulación psicológica para obtener información confidencial.	El atacante se hace pasar por alguien de confianza (técnico, colega, proveedor).	Obtener contraseñas, claves o información privada mediante engaño.	Alta frecuencia en entornos contables por la confianza entre áreas o con clientes.	Kovacevik, 2025; Kaspersky, 2025

Nota. Datos recopilados por el autor, las referencias se encuentran detalladas dentro de la misma tabla.

El daño que causan este tipo de ciberataques, informa *Cybersecurity Ventures* (2024), es bastante mayor y el costo del ciber crimen se estima en unos 10.95 billones de dólares en este año 2025, lo cual lo convierte en la actividad ilícita más lucrativa del mundo.

Por otra parte, los riesgos calculados son un tema importante que ha hecho crecer a la industria de la protección, generando un aparente sinfín de contrapropuestas a cada posibilidad de ciberataque, éstas van desde los clásicos an-

tivirus y firewalls, hasta software más complejo. Revisemos la lógica de este software.

Tabla 3

Herramientas de ciberseguridad aplicadas a la contaduría.

Herramienta o sistema	Descripción general	Función principal	Ventajas destacadas	Relevancia en el ámbito contable
Firewalls	Barreras de seguridad que bloquean actividades sospechosas en redes.	Filtrar y controlar el tráfico de red, evitando accesos no autorizados.	Protección preventiva ante intentos de intrusión o robo de datos.	Resguardan información sensible y financiera almacenada en servidores contables.
Antivirus y antimalware	Programas diseñados para detectar y eliminar software malicioso.	Identificar, poner en cuarentena y eliminar virus o malware.	Actualizaciones constantes para enfrentar nuevas amenazas.	Protegen bases de datos contables y sistemas administrativos frente a infecciones.
Detección y respuesta de *endpoints* (EDR)	Sistemas que monitorean dispositivos y detectan comportamientos anómalos.	Analizar actividad en *endpoints* y responder a amenazas en tiempo real.	Monitoreo continuo y capacidad de respuesta automatizada.	Mantienen seguros los equipos de trabajo contable conectados a red.
Software de ciberseguridad empresarial	Soluciones avanzadas que integran análisis en tiempo real, IA y aprendizaje automático.	Proteger información corporativa con múltiples capas de seguridad.	Integración de IA, análisis predictivo y protección en la nube.	Adecuado para firmas contables que manejan grandes volúmenes de datos financieros.

Nota. Datos elaborados por el autor a partir de información de IBM (2025).

3.8. Herramientas de seguridad contable

Herramientas SIEM/SOAR: SIEM (gestión de eventos e información de seguridad, por sus siglas en inglés) / **SOAR** (orquestación de seguridad, automatización y respuesta, por sus siglas en inglés): Son herramientas de ciberseguridad que correlacionan información para detectar y dar respuesta a incidentes. En términos contables, la información que protege es de libros contables, permite detectar cambios en controles de cuentas, movimientos y transacciones sospechosas y conserva evidencias de las auditorías (*Splunk*, 2025). Dos productos representativos de estas herramientas son *Splunk Enterprise Security* y uno bastante famoso que es el *Microsoft Sentinel.*

Herramientas EDR/XDR: Anteriormente vimos lo que es EDR en términos de detección y respuesta en endpoints o dispositivos, XDR dignifica *extended detection and response*, lo cual lo vuelve un trabajo de amplio alcance (se puede decir que EDR observa dispositivos individuales y XDR se apertura hacia la infraestructura de seguridad que puede incluir a la nube, las redes adyacentes, cuentas de correo electrónico, servidores, etc.). Al ser un trabajo en medida extensa, puede hacer una telemetría que pueda aislar dispositivos para que no sigan siendo atacados, realizar la "cacería" del intruso en caso de haberlo y operar un MTR (de *Managed threat response*, que es respuesta de manejo de la amenaza), que establece un reporte de seguimiento de la misma y la posible fuente de la que proviene (*CrowdStrike*, 2025). Una EDR muy usada es *CrowdStrike Falcon* y en Estados Unidos es famosa en niveles corporativos. Una XDR empresarial útil es Palo Alto *Cortex XDR*.

Herramientas de gestión de identidad: IAM (*Identity & Access Management*) y MFA (*Multifactor Authentication*): Este tipo de herramientas permiten la gestión segura de autenticación de cuentas. Este tipo de herramientas ayuda mucho en la contabilidad de algún negocio, incluso para el manejo corporativo, ya que controla la aprobación de pagos, modifica proveedores o exportar reportes. Así mismo, entre la autorización y la negación de accesos, permiten gestionar cuentas de usuarios por nivel jerárquico o importancia del mismo, generando protección única (CyberArk, 2025). *Okta Identity Club* es un software empresarial que es de utilidad para proteger accesos a sistemas contables en la nube a través de diversos niveles de autenticación (Okta, s/f).

PAM (*Privileged Access Management*) para gestión de cuentas privilegiadas: Gestiona y audita cuentas con privilegios, tales como cuentas de administradores, accesos de jefes corporativos e incluso de los propios manejadores de los servicios digitales. Se basa principalmente en bóvedas de contraseñas, cada inicio de sesión queda grabado y los accesos son controlados en solicitudes y aprobación, además de ser susceptibles de ser auditados. En contabilidad nos queda claro que este tipo de cuidados son óptimos para el movimiento de activos, manipulación de conciliaciones, aprobación de pagos, etc. (*CyberArk*, 2025). Esta es una de las herramientas que el profesional contable debe considerar como un punto de seguridad necesario y conocerlo a fondo. *CyberArk Privileged Access Manager* es un software de protección de credenciales y útil en auditar actividad de los usuarios.

Herramientas para la prevención de pérdida de datos y protección de datos sensibles: DLP (prevención de pérdida de datos) /DSPM (Gestión de la postura de seguridad

de datos: Como su nombre lo dice, estas herramientas son específicas para detectar, bloquear o restringir el movimiento de datos sensibles para evitar filtraciones y para generar un informe de daños. En contabilidad los beneficios están claros. Desde proteger bases de datos financieros hasta evitar fugas que puedan causar pérdidas económicas, este tipo de protección se especializa en la prevención y cuidado de los datos (Forcepoint, 2025). La herramienta *Forcepoint Data Loss Prevention* es un software ideal para la prevención y detección en tiempo real.

Herramientas para la visibilidad y comportamiento de usuarios: Data security/DSPM/UEBA (Análisis de conductas de usuarios y entidades por sus siglas en inglés): Este tipo de herramientas suele usar aprendizaje automático o *machine learning* para la detección de anomalías. Como ya explicamos arriba el DSPM, cabrá completar que el trabajo que ofrecen estas herramientas es de seguimiento de datos sensibles, como siguiendo un rastro de los mismos. Si existen amenazas o comportamientos anómalos, la IA los seguirá para saber si existen amenazas internas de las qué ocuparse. Varonis es un programa que ayuda a descubrir, clasificar y analizar comportamiento en datos corporativos. Su uso en contabilidad también incluye detección de accesos masivos a carpetas de nómina o cambios poco comunes en libros contables (Varonis, 2025).

Herramientas de control y protección de SaaS (software como servicio por sus siglas en inglés) y acceso web: CASB (agente de seguridad de acceso a la nube, por sus siglas en inglés) /SWG (Gateway web seguro, es decir, una entrada a internet que sea segura evitando malware y otros ataques): Todo software usado en línea (uno muy común es *Google Docs* que se aloja en el Drive, por ejemplo), corre riesgo de ser intervenido maliciosamente o simplemente

tiene que ser protegido para que esa información no sea pública o sean descargados sus datos por terceros. En el uso contable, es común que se usen apps como *QuickBooks Online, Xero,* o Excel y un sistema CASB evita que sus datos sean compartidos indebidamente. *Zscaler* es un software bastante eficiente para la protección de esas apps y el tráfico web de los usuarios (Zscaler, 2025).

Protección contra los fraudes por correo electrónico: E mail security/ *Anti phishing* (BEC, correo electrónico empresarial comprometido por sus siglas en inglés): Es un filtrado avanzado para evitar el *phishing*, que como apuntábamos en la sección anterior, adquiere formas más complejas como el *spear phishing*, el cual, usando una combinación de ingeniería social y mensajes personalizados, busca conseguir información de acceso privado (Akamai, 2025). Son engaños más creíbles por ser exactamente dirigidos al individuo para lucir más legítimos. El BEC permite detectar ese tipo de engaños protección contra el llamado *CEO impersonation* que es una forma de suplantar a alguna autoridad y girar órdenes para realizar un fraude contable y robos de pagos (*Proofpoint*, 2025). Algunos nombres de software adecuado para detectar este tipo de ataques son el *Proofpoint y Mimecast* (Mimecast, s/f).

Herramientas para controles de gobierno, riesgo y cumplimiento: GRC/ERP (Planificación de recursos de la empresa, por sus siglas en inglés): Este grupo de herramientas es bastante amplio ya que involucra amplios controles muy específicos y puede haber prevención en todos ellos en varios niveles, como ya hemos visto en este apartado. Sin entrar en demasiados tecnicismos, podemos decir que estas herramientas buscan automatizar controles, gestión de riesgos, evidencia y auditoría continua (SAP, s/f). Ya hemos visto otras herramientas que ejercen este tipo de

trabajos, pero en conjunto, podemos hablar de algunos softwares como Oracle y Microsoft Dynamics pueden incluir este tipo de herramientas. Queremos hacer notar que existe mucha oferta ya que, al momento de realizar las búsquedas para esta investigación, de herramientas de gestión llegaba al número de casi cien ofertas diferentes, lo cual también habla de que este, es todo un sector de la industria digital de entre muchas otras herramientas dentro del apartado de ciberseguridad.

Herramientas de Backup/Ransomware resilience, (copias inmutables y recuperación): En la búsqueda de recuperar archivos perdidos o destruidos, siempre es necesaria la posibilidad de una herramienta de respaldos regulares y automatizados, cifrados y verificación de integridad, al grado de tener posibilidad de recuperar balances o archivos contables. Hay software como *Veeam Backup and Replication,* que da muchas opciones de portabilidad y formas de recuperación de los archivos perdidos (Veeam, 2025).

Herramientas de monitoreo de integridad de aplicaciones y bases de datos: Estas herramientas son eficaces para el cambio masivo de esquemas en bases de datos críticas, también permiten hacer exportación masiva de datos y vigilar el proceso, emitiendo alertas cuando se detecta alguna anomalía durante el monitoreo. En contabilidad ayuda a resguardar y trasladar libros mayores, cuentas y planillas de pago. Uno de los softwares más usados es el IBM Guardium (IBM, 2025) o el Imperva.

Hasta este punto hemos podido ver los problemas de seguridad más comunes y recurrentes y parte de las soluciones que se otorgan por el lado de comerciantes de software de seguridad, sobre todo en el contexto contable. El problema de la ciberseguridad, como mencionamos al inicio

del apartado, es millonario y preocupante, y supone un negocio redondo tanto en lo ilícito como en lo lícito. Las licencias de software se mueven constantemente en los ambientes empresariales y han significado un proceso de aprendizaje para los involucrados, ya que se puede notar según las descripciones realizadas, que no sólo está involucrado el personal de apoyo técnico o departamento de informática, también el usuario profesional como lo es el contable, debe tener la preparación para el manejo de estas herramientas, ya que lo complejo del tema es hacia dónde se dirigirá el nivel de protección deseado, por lo que entra en acción el tema de la formación en esta área, lo cual ya significa considerar recursos y tiempo activos para el despliegue de cuanto sea necesario cubrir. Todo lo revisado hasta el momento, se relaciona fuertemente con el área contable, pero las organizaciones y empresas, no importa el tamaño, involucran también a otros profesionistas y eso ha de tomarse en cuenta; al final, por lo que abogamos, es por un trabajo conjunto a la vez que un esfuerzo constante de manera grupal que sea sensible a los cambios y necesidades de la seguridad en la organización.

Se debe prestar atención en cómo se plantea el desafío de seguridad, haciéndolo de una manera latente, silenciosa pero presente en muchos de los campos financieros a los que volteemos a ver. La cobertura noticiosa es lenta y parece explorar si llama la atención del público, pero no por eso significa que sea un mal menor. El punto es que hay que informarse como público y como profesionistas. El prevenir ataques cibernéticos también involucra cuestionar a quienes "gobiernan" los algoritmos y las decisiones automatizadas que se desprenden de ellos (recordemos el fenómeno *black box*) y hasta qué punto la ética profesional se puede mantener en los entornos digitales, sobre todo, porque debemos pensar en quiénes manejan dichos

entornos. Como vimos a través del capítulo, el reconocimiento que queda claro, es que la ciberseguridad y la gestión ética de los datos son riesgos del presente y son de primer nivel. La contaduría, que posee un prestigio que recae en la confianza, la vulneración de estas áreas representa un reto vigente del que ninguno de los profesionales puede escapar.