



SILVIA LEAL,
presidenta del Colegio de Contadores

“La sofisticación de las estafas obliga a incorporar la seguridad digital como parte de la gestión cotidiana”

En los últimos años, con el avance de la digitalización y la sofisticación de los fraudes, la ciberseguridad se convirtió en uno de los mayores desafíos para las empresas y los profesionales contables. A esto se suman los cambios que implicó la inteligencia artificial (IA), la necesidad de fortalecer la prevención de los delitos financieros y los reclamos por una mayor simplificación de los trámites administrativos. Acerca de estos temas, que ocupan un lugar cada vez más importante en la agenda del Colegio de Contadores, Economistas y Administradores del Uruguay (Cceau), dialogó con *La Mañana* su presidenta, Silvia Leal.

¿Qué tan preparados están hoy los estudios contables y las empresas en Uruguay para enfrentar estafas y delitos financieros, que son cada vez más sofisticados?

Hoy existe una conciencia mucho mayor sobre los riesgos de estafas, fraudes y delitos financieros. Las empresas y los estudios contables han avanzado en digitalización, pero muchas veces la seguridad no ha crecido al mismo ritmo. El profesional está en una posición especialmente sensible, maneja información económica, tributaria, bancaria, societaria y laboral de sus clientes. Eso lo convierte en un actor clave para prevenir riesgos, pero también en un posible objetivo de intentos de fraude.

El gran desafío es pasar de una actitud reactiva a una preventiva. No alcanza con actuar cuando el daño ya ocurrió. Hay que fortalecer controles, capacitar equipos, revisar procesos internos y generar hábitos de verificación. La sofisticación de las maniobras obliga a que profesionales y empresas incorporen la seguridad digital como parte de la gestión cotidiana.

¿Cuáles son los mayores desafíos vinculados a la seguridad digital actualmente?

Los principales desafíos están en tres planos: tecnológico, humano y organizacional. En lo tecnológico, aparecen riesgos vinculados al acceso remoto, uso de plataformas en la nube, resguardo de contraseñas, respaldos de información, correos electrónicos falsos y operaciones digitales cada vez más difíciles de verificar.

Pero el factor humano sigue siendo decisivo. Muchas estafas no ingresan por una falla del sistema, sino por un correo convincente, una identidad suplantada, una urgencia simulada o una instrucción falsa de pago. Por eso la capacitación permanente es fundamental.

Y en lo organizacional, el desafío es que las empresas, especialmente las pequeñas y medianas, incorporen protocolos mínimos como doble validación para pagos, segregación de funciones, controles sobre cambios de cuentas bancarias, respaldo documental suficiente y revisión periódica de accesos.

En un reciente comunicado, el Cceau advirtió que el avance de la digitalización incrementó los riesgos asociados a fraudes informáticos, documentación falsa, suplantación de identidad y operaciones vinculadas a activos virtuales. En ese sentido, ¿qué deben hacer los

profesionales para evitar caer en esas trampas?

Lo primero es no naturalizar la urgencia. Muchas maniobras fraudulentas se construyen sobre la presión: "pagá ahora", "cambía esta cuenta", "firmá este documento" o "ingresá a este enlace". Frente a eso, el profesional debe detenerse, verificar y documentar.

También es clave fortalecer la debida diligencia del cliente, conocer el origen de fondos, identificar beneficiarios finales, revisar documentación respaldante y estar atentos a inconsistencias. En operaciones con activos virtuales, documentación digital o identidades no presenciales, el estándar de cuidado debe ser mayor.

El contador no puede limitarse a recibir información y procesarla mecánicamente. Debe aplicar criterio profesional. La tecnología ayuda, pero no sustituye la responsabilidad de analizar si una operación es razonable, consistente y respaldada.

Con el avance de la IA, ¿qué ha cambiado para el trabajo de los contadores? ¿Qué sigue dependiendo sí o sí del criterio humano en esta profesión?

La IA ya está cambiando la profesión. Automatiza tareas, permite analizar grandes volúmenes de información, detectar patrones, mejorar procesos y reducir tiempos operativos. Pero también abre nuevos riesgos, por ejemplo, documentos falsos más verosímiles, identidades simuladas, correos más sofisticados y fraudes más difíciles de detectar.

Lo que sigue dependiendo del criterio humano es lo esencial, es decir, interpretar, contextualizar, decidir, advertir riesgos y asumir responsabilidad profesional. La IA puede apoyar el trabajo, pero no reemplaza la ética, el juicio profesional ni la comprensión integral del negocio.

El contador del futuro no será menos necesario; será necesario de otra manera. Deberá saber utilizar herramientas tecnológicas, pero también mantener una mirada crítica. La confianza, la responsabilidad y la independencia profesional no se automatizan.

Por otra parte, el Cceau señaló que todavía existe un amplio margen para simplificar trámites administrativos, especialmente para pequeñas y medianas empresas. ¿Cuáles son los procesos que hoy generan más pérdida de tiempo para las empresas y los profesionales y qué es lo que plantean para resolverlo?

En Uruguay todavía hay un margen muy importante para simplificar trámites. Las pequeñas y medianas empresas destinan demasiado tiempo y recursos a cumplir obligaciones dispersas, repetidas o poco coordinadas entre organismos. Muchas veces se solicita información que el propio Estado ya posee, pero que debe volver a presentarse en otro formato, ante otra oficina o en otro sistema.

Entre los procesos que generan más carga están la duplicación de información contable y financiera, los trámites ante distintos organismos, las exigencias formales repetidas, la



"En lo organizacional, el desafío es que las empresas, especialmente las pequeñas y medianas, incorporen protocolos mínimos de ciberseguridad"

falta de interoperabilidad entre plataformas y la inestabilidad de algunos sistemas en momentos críticos de vencimientos.

Desde el Cceau planteamos avanzar hacia un Estado más coordinado, con sistemas confiables, información reutilizable y criterios previsibles. La Central de Balances debería consolidarse como un verdadero repositorio único de estados financieros, evitando que los profesionales deban preparar información similar para bancos, organismos públicos y otros usuarios.

Simplificar no es bajar controles. Es controlar mejor, con menos duplicación y más inteligencia. Para las empresas, especialmente las pymes, cada hora destinada a trámites innecesarios es una hora menos para producir, innovar o generar empleo.

¿Qué papel cumple el colegio en estos temas?

Estamos frente a una transformación profunda del ejercicio profesional. La digitalización, la IA, la prevención de fraudes y delitos financieros y la necesidad de simplificar la relación entre las empresas y el Estado forman parte de una misma agenda. El profesional en ciencias económicas cumple hoy un rol estratégico para la confianza económica. No solo procesa información, sino que la interpreta, identifica riesgos, acompaña la toma de decisiones y contribuye a la transparencia, la formalización y la sostenibilidad de las organizaciones.

Por eso, desde el Cceau insistimos en tres pilares fundamentales: la capacitación permanente, el diálogo técnico e institucional con las autoridades y la defensa del ejercicio profesional. Uruguay necesita profesionales preparados, empresas protegidas y un Estado que facilite el cumplimiento y promueva la competitividad.

La prevención frente a los delitos informáticos, el fraude y el lavado de activos no depende únicamente de la tecnología, sino también de contar con profesionales actualizados, capaces de reconocer señales de alerta, aplicar procedimientos adecuados y actuar con criterio profesional frente a riesgos cada vez más sofisticados.

En ese contexto, el Cceau desempeña un papel clave para los profesionales. Es la institución que de manera permanente alerta sobre nuevas modalidades de estafa y fraude, difunde información técnica actualizada y brinda formación continua en las distintas áreas de incumbencia profesional, incluyendo la prevención de delitos financieros y riesgos digitales. Los ciberdelincuentes innovan todos los días, por eso, mantenerse informado y capacitado ya no es una opción, es una necesidad. Contar con una institución que represente, informe, capacite y acompañe a los profesionales resulta hoy más valioso que nunca. Y hacerlo a través de una cuota accesible demuestra que la inversión en formación, respaldo institucional y defensa profesional tiene un retorno directo para quienes ejercen la profesión y para la sociedad en su conjunto.