

En Valencia a 07 de octubre de 2024

El auditor Luis Vilanova Blanco con DNI 22570043M, colegiado nº 498 por el Colegio Oficial de Ingenieros en Informática de la Comunidad Valenciana (COIICV), auditor **certificado CISA por ISACA con ID CISA-18144709**, master en **CIBERSEGURIDAD** por Deloitte, formado en **ISO27001** por SGS e **ISO27017** por BSI, miembro de la Asociación de **Peritos Colaboradores con la justicia** de Madrid y Valencia, así como de la Asociación Profesional Colegial de Peritos Judiciales del Reino de España y de la Asociación Profesional de Peritos Judiciales colaboradores con la Administración de Justicia peninsular, insular y de las ciudades autónomas de España, así como **colaborador con la Asociación Profesional de Asesores Fiscales**, fundador de www.leyantifraude.com, auditor de digitalización certificada de facturas ante la **agencia tributaria**, principal auditor de **receta médica privada electrónica** en España ante la Organización Médico Colegial, auditor de slots de **juegos y apuestas online basado en la ISO27001**, comparezco y como mejor proceda en derecho.

Digo:

En relación con la solicitud de auditoría y consultoría de adaptación a la Ley Antifraude Artículo 201 bis ley 11-2021 aplicable al software CMW versión 16.0.0 de la empresa Colegio Profesional de Administradores de fincas de Madrid, con CIF G-28840387 resuelvo presentar el siguiente dictamen que recoge el resultado de las diligencias que se demandaban.

Una vez analizado el proyecto, aseguro que este programa informático dispone de medidas de integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros y que dicho programa ha sido **objeto de 29 ajustes revisados, de los cuales 21 de ellos se han realizado/modificado por ser aplicables en dicho software** para aumentar al máximo el cumplimiento legal.

En la siguiente tabla se realiza un resumen del nivel alcanzado de cumplimiento en los cuatro primeros epígrafes de la ley según la siguiente categorización de riesgo residual y **teniendo en cuenta que el riesgo nulo no existe**.

Muy bajo: Una vez implantadas las medidas recomendadas la realización de caja B y/o facturación en paralelo o bien no cumplir con la Ley Antifraude en alguno de sus epígrafes no resulta viable para el obligado tributario, estando el sistema generalmente en modalidad Cloud o Cloud SaaS bajo el control del proveedor.

Bajo: Una vez implantadas las medidas recomendadas la realización de caja B y/o facturación en paralelo o bien no cumplir con la Ley Antifraude en alguno de sus epígrafes resulta poco viable para el obligado tributario excepto si es capaz de violar las medidas de seguridad de la implantación o bien acceder mediante diferentes técnicas a la base de datos. Esta situación se debe fundamentalmente al estar ante una arquitectura **On Premise** donde el obligado tributario dispone del sistema de base de datos a su disposición en modo edición, **caso que nos ocupa**.

Alto: Una vez implantadas las medidas recomendadas la realización de caja B y/o facturación en paralelo o bien no cumplir con la Ley Antifraude en alguno de sus epígrafes resulta viable para el obligado tributario una vez conozca el modo de funcionamiento del programa o bien la arquitectura y medidas de seguridad implantadas.

Muy alto: Una vez implantadas las medidas recomendadas la realización de caja B y/o facturación en paralelo o bien no cumplir con la Ley Antifraude en alguno de sus epígrafes resulta viable para el obligado tributario con facilidad.

Nivel	Riesgo residual
1. Intencional.	Bajo
Funcionalidades que podrían ser interpretadas por el órgano sancionador que intencionalmente permitan las malas prácticas que a su vez habiliten situaciones de fraude o caja B. Por ejemplo, supongamos que la creación y borrado de una empresa no deja rastro en el software, permitiendo trabajar con contabilidades en paralelo, entre otros...	
2. Mala práctica por diseño.	Bajo
Aquel software que permita manipulaciones no pensadas estrictamente para el fraude pero sí que podría ser aprovechado por el usuario, como por ejemplo eliminar una factura ya enviada o impresa, en un estado de ya emitida y registrada, entre otros...	
3. Por ausencia de controles.	Bajo
Supongamos que una instalación puede accederse directamente y saltando toda la seguridad a los datos almacenados en la base de datos y en una factura modificar los importes, sin dejar rastro ni alerta de esa alteración de una transacción ya realizada, entre otros...	

Se recomienda:

1. El paso de sus implantaciones a versión Cloud SaaS para minimizar aún más el riesgo de fraude.
2. Finalizar el cumplimiento del reglamento cuando este publicado definitivamente, obligando al uso de VERIFACTU en sus clientes.

Y para que así conste expido el presente, asegurando que no comprenden las incompatibilidades generales de la ley, declarando bajo juramento que he dicho toda la verdad y actuado con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes implicadas, conociendo las sanciones penales en las que podría incurrir si incumpliere dicho deber como perito.

Tanto auditor como empresa desarrolladora juran haber actuado diciendo la verdad en la documentación y conclusiones intercambiadas, quedando, según la opinión de este auditor un nivel residual de riesgo en el momento que la empresa desarrolladora implementa el plan de acción.

Siendo este mi criterio que someto a otro mejor fundado en Valencia, a fecha de emisión de este informe.

