Documento adhesión para clientes, distribuidores y partners.

RESPONSABILIDAD DEL OBLIGADO TRIBUTARIO

Contenido

SOFTWARE CAFMADRID APLICACIÓN CMW

1. Introducción

La Ley 11/2021 de 9 de julio, que se publicó en el Boletín Oficial del Estado el 10 de julio, introduce medidas para prevenir y combatir el fraude fiscal, adaptar la legislación tributaria a la normativa europea, y regular el juego. Esta ley entra en vigor gradualmente desde el 11 de julio de 2021.

Entre sus disposiciones, el Artículo 201 bis establece que es infracción tributaria fabricar, producir y comercializar sistemas y programas informáticos o electrónicos que se usen para la contabilidad, la facturación o la gestión de actividades económicas, cuando se den alguna de estas situaciones:

a) Permitan llevar contabilidades diferentes, según el artículo 200.1.d) de esta Ley.
b) Permitan no registrar, total o parcialmente, las operaciones realizadas.
c) Permitan registrar operaciones distintas a las que se han realizado.
d) Permitan modificar operaciones ya registradas, incumpliendo la normativa vigente.
e) No cumplan con las especificaciones técnicas que aseguren la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros, así como su legibilidad por parte de los órganos competentes de la Administración Tributaria, de acuerdo con el artículo 29.2.j de esta Ley.
f) No se certifiquen, cuando sea obligatorio por reglamento, los sistemas fabricados, producidos o comercializados.

También es infracción tributaria tener los sistemas o programas informáticos o electrónicos que no se ajusten a lo que dice el artículo 29.2.j) de esta Ley, cuando no estén debidamente certificados y tengan que estarlo por reglamento, o cuando se hayan alterado o modificado los dispositivos certificados.

2. Responsabilidades

Resaltamos que fabricante, distribuidor o cliente deben cumplir con la ley que les afecta. Como partner/fabricante de software CMW trabajamos para mejorar nuestro software en cumplimiento y formar a nuestros comerciales y distribuidores. En cuanto al cliente (OBLIGADO TRIBUTARIO), quien usa nuestro software, tiene responsabilidades y obligaciones derivadas de esta ley, **que no son responsabilidad del fabricante del software, sino del cliente**. A continuación, explicamos las responsabilidades clave del cliente (colegiado titular de la licencia de uso) de nuestro software.

1. Políticas de copias de seguridad

Los clientes deben hacer backups (Copias de Seguridad) de su software siguiendo unas normas establecidas, que tengan en cuenta las buenas prácticas del sector, como:

- Hacer backups firmados, con clave, en dos lugares y medios distintos y conservarlas de forma segura.
- Tener un registro de acceso o modificación de los backups.

2. Políticas de retención de información

La política de copia de seguridad establece que se deben configurar las copias de reserva siguiendo estas normas y principios:

- Guardar al menos una copia anual de los últimos cuatro ejercicios fiscales obligatorios por ley.
- Hacer copias diarias, semanales, mensuales y anuales de facturas (MAID) y de eventos del sistema.
- No se permite eliminar la empresa del OBLIGADO TRIBUTARIO.

3. Políticas de actualización de sistemas y versiones

Se debe actualizar el software del sistema operativo y otros como el motor de base de datos para evitar vulnerabilidades que afecten la conservación legal.

El OBLIGADO TRIBUTARIO se compromete a tener la aplicación actualizada siempre en la última versión publicada de software.

4. Clonado de la instalación

No se permite clonar la instalación para crear una empresa, facturación o caja paralelas que puedan violar la ley antifraude, por lo que los datos clonados desde un espacio de trabajo licenciado no podrán usarse.

5. Políticas de contraseñas

La política de contraseñas establece los siguientes requisitos para las contraseñas:

- Las contraseñas deben ser robustas (al menos 8 caracteres, con minúsculas, mayúsculas y números).
- Se recomienda modificar la contraseña como mínimo dos veces al año.
- No se recomienda usar versiones de contraseñas anteriores (por ejemplo, agregando un número a una contraseña vieja)
- Aconsejamos el uso de gestores de contraseñas.

6. Políticas de control de acceso

Esta política se aplica a todo el personal, tanto interno como externo, y se recomienda que el acceso se conceda según el principio de necesitar saber/necesitar usar.

El acceso a la información/activo depende del rol de la persona.

El "colegiado/supervisor" es el responsable de conceder o revocar el acceso. El usuario puede pedir el acceso por su cuenta, pero la solicitud tiene que ser validada primero por el "colegiado/supervisor".

Los derechos de acceso también se conceden o revocan como parte del proceso de incorporación o de cese de "Recursos Humanos".

Para sistemas con información sensible (según la Política de clasificación de la información), se debe usar 2FA (Autenticación de dos factores) siempre que sea posible.

Las ID's de usuario no se pueden reutilizar para sistemas que contienen información confidencial o sensible.

Requisitos para sistemas de contraseñas:

- Se pide al usuario que cambie la contraseña por defecto en el primer acceso.
- Se debe exigir al usuario que use contraseñas de calidad (según la Política de contraseñas)
- No se deben reutilizar las tres contraseñas anteriores.
- Las contraseñas se deben guardar de forma segura (cifradas/hashed/separadas de otros datos)
- La información de acceso se debe enviar cifrada (usando TLS).

7. Política criptográfica

El OBLIGADO TRIBUTARIO tiene la obligación de mantener y renovar el certificado electrónico y la clave que usa para la firma electrónica de los registros de facturación y/o para la comunicación con las administraciones públicas, entre otras, agencia tributaria y la Seguridad Social.

El OBLIGADO TRIBUTARIO tiene la obligación de vigilar la caducidad del certificado y de actualizarlo junto con su clave cuando sea necesario.

Establece cuándo, dónde y cómo se emplea la criptografía en nuestra organización, y cómo se gestiona la administración de claves. Por ejemplo, para la firma digital de facturas y logs así como el cifrado de copias de seguridad.

Algunos requisitos:

- Duración máxima para la firma de certificados es 1 año
- La duración máxima de los certificados SSL/TLS es 2 años
- El uso de “wildcar certificates” no está permitido
- Todos los certificados deben tener una longitud de clave de al menos 2048 bits o superior.
- Todos los certificados deben gestionarse a través de la gestión de activos en Certificados.

8. Política de malware y antivirus

El OBLIGADO TRIBUTARIO tiene la responsabilidad de contar en sus sistemas informáticos con medidas que reduzcan la posibilidad de entrada de virus o cualquier tipo de malware que pudiera dañar aspectos como la conservación o integridad de la información, según lo establecido por la ley.

El OBLIGADO TRIBUTARIO se compromete a implementar controles de detección, prevención y recuperación para protegerse del malware, junto con el adecuado conocimiento del usuario.

En concreto:

- Instalar herramientas antivirus / antimalware (y verificar que estén actualizadas)
- Evitar que los usuarios instalen software sin autorización.
- Controles de red para evitar la descarga o ejecución de malware.
- Sensibilización y formación proactiva a los usuarios sobre malware.
- Segregación en redes.

9. Política de sincronización fecha y hora

El OBLIGADO TRIBUTARIO debe asegurarse de que la fecha y hora de su dispositivo estén bien sincronizadas, ya que tanto el sistema de facturación, contabilidad, gestión y VERI*FACTU usarán la fecha y hora para asignarlas.

10. Política de acceso a Internet VERI*FACTU

Es responsabilidad del OBLIGADO TRIBUTARIO contar con acceso a internet para la correcta comunicación de las facturas VERI*FACTU.

11. Política de uso de VERI*FACTU

El sistema de comunicación VERI*FACTU está protegido, garantizado, y no se puede modificar sin la supervisión del Colegio de Administradores de Fincas de Madrid (CAFMADRID). El sistema que hace funcionar VERI*FACTU y por tanto asegura el flujo de comunicación según las especificaciones técnicas no se puede parar y tiene que estar en funcionamiento el 100% del tiempo. Se recuerda la obligatoriedad de añadir los ficheros generados por VERI*FACTU, incluido todos los datos de comunicación, respuesta, logs, etc. los años con responsabilidad del obligado tributario.

12. Política de sincronización SII

CMW no admite ni da soporte a Clientes incluidos en este régimen. El SII es obligatorio para aquellas empresas que tengan un volumen de facturación superior a los 6 millones de euros, o que estén acogidas al régimen especial del grupo de entidades del IVA/IGIC o que estén inscritas en el Registro de Devolución Mensual del IVA/IGIC (REDEME).

13. Política de cierre de periodo

EL OBLIGADO TRIBUTARIO debe asegurarse y es responsable de no modificar operaciones ya registradas. Esto es esencial para cumplir con la normativa vigente. En el caso de necesitar reabrir un ejercicio o periodo para realizar algún ajuste contable justificado, es importante seguir los procedimientos adecuados. Incumplir esta normativa puede tener consecuencias graves. Por favor, asegúrese de seguir estas pautas en todo momento.

14. CMW ON PREMISE

CMW se instala ON PRIMISE, por ello, EL OBLIGADO TRIBUTARIO debe asegurarse y es responsable de no modificar la base de datos si tuviera conocimiento para ello. Esto es esencial para cumplir con la normativa vigente y mantener la licencia de uso. En el caso de necesitar realizar algún proceso justificado de reparación en la BD, debido a algún mal funcionamiento, corte en la aplicación, etc. que haya dañado o duplicado algún dato, deberá contactar con el servicio de atención al cliente y seguir los procedimientos adecuados. Incumplir esta normativa puede tener consecuencias graves. Por favor, asegúrese de seguir estas pautas en todo momento.

3. Declaración de responsabilidad

CAFMADRID como partner y fabricante de software y **No siendo el usuario final,** se compromete a ofrecer herramientas informáticas y procedimientos seguros que minimicen el riesgo de uso fraudulento de nuestro software.

Sin embargo, clientes, partners y distribuidores son responsables de no usar o realizar ninguna acción que busque hacer caja B, facturación en paralelo o incumplir la ley, ni de modificar o desarrollar informáticamente nada que afecte a las medidas de seguridad y cumplimiento de la ley.

El sistema se instala on premise, el usuario no tiene información alguna de acceso y desbloqueo de la base de datos, siendo el propio partner fabricante del software quien, para una hipotética reparación, si fuera necesario el acceso justificado puede acceder previa copia de seguridad facilitada por el usuario, quedando trazabilidad de dicha intervención.

4. Adhesión

Declaro haber leído el Documento de adhesión para el uso del software CMW en su versión a partir de la 16.0.0, el cual permite velar por el cumplimiento de la nueva ley antifraude, incluyendo controles y medidas de seguridad de forma continua en un plan de acción de mejora continua en constante evolución.

Asimismo **como usuario final (obligado tributario)** adquiero el compromiso expreso de llevar a cabo el conjunto de operaciones de seguridad y buenas prácticas descritas anteriormente en este documento de adhesión orientado al cumplimiento de Artículo 201 bis, Ley 11/2021, 9 de julio, con el fin de no permitir la facturación en paralelo, caja B o incumplimiento de la misma.