



# LIBRA

EVENT DRIVEN ENTERPRISE

**DOCUMENTO  
INFORMATIVO PARA  
PARA EL CUMPLIMIENTO  
DE LA LEY 11/2021**

**LIBRA**

**EDISA**  
CENTRO DE INNOVACION

## Índice

1. Introducción .....	3
2. Responsabilidades de la empresa usuaria LIBRA .....	5
2.1 Uso de LIBRA acorde a lo establecido en la Ley .....	5
2.2 Política de copias de seguridad .....	5
2.3 Políticas de actualización de sistemas.....	7
2.4 Políticas de contraseñas.....	8
2.5 Políticas de control de acceso .....	8
2.6 Política criptográfica .....	9
2.7 Política malware y antivirus .....	9
2.7 Continuidad de las operaciones y del negocio de la empresa.....	10
3. Declaración de haber sido informado de las responsabilidades de la empresa .....	11

# 1. Introducción

El objetivo de este documento es establecer las responsabilidades asociadas al cumplimiento del Artículo 201 bis, de la Ley 11/2021, del 9 de julio de 2021 a la que nos referiremos como Ley Antifraude.

En concreto el Artículo 201 bis establece que es una infracción tributaria la producción, comercialización y tenencia de sistemas informáticos que soporten los procesos contables, de facturación o de gestión, que no cumplan las especificaciones exigidas por la normativa aplicable. En concreto, se incurrirá en infracción tributaria cuando concurren cualquiera de las siguientes circunstancias:

- a) Que el software permita llevar contabilidades distintas en los términos del artículo 200.1.d) de esta Ley.
- b) Que el software permita no reflejar, total o parcialmente, la anotación de transacciones realizadas.
- c) Que el software permita registrar transacciones distintas a las anotaciones realizadas.
- d) Que el software permita alterar transacciones ya registradas incumpliendo la normativa aplicable.
- e) Que el software no cumpla con las especificaciones técnicas que garanticen 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, en los términos del artículo 29.2.j) de esta Ley.
- f) Que no se certifiquen, estando obligado a ello por disposición reglamentaria, los sistemas fabricados, producidos o comercializados.

Es importante subrayar que tanto fabricante, distribuidor o cliente tienen responsabilidades que afectan al marco de cumplimiento de esta ley. Como fabricante del software ERP LIBRA, EDISA ha llevado a cabo una auditoría a través de una empresa auditora independiente, para identificar los aspectos que se requieren de forma específica en esta Ley, llevando a cabo todos los cambios que han sido indicados en esta auditoría, con el objetivo de alcanzar el máximo nivel de cumplimiento.

Es importante destacar que esta Ley hace referencia a un reglamento que está en fase de revisión y que definirá entre otros aspectos los requisitos que deben cumplir las facturas a partir de una determinada fecha, entre los que ya se señalan algunos como el de incorporar una codificación QR o la de generar un hash encadenado que evite la modificación de las facturas una vez emitidas.

LIBRA está adaptado a las exigencias de la administración electrónica en los países en los que está implantado y en concreto en España, LIBRA incorpora como parte del propio software la comunicación con distintos sistemas de la administración pública, entre los que puede citarse el sistema FACE, el TicketBai y por supuesto el Sistema de Suministro Inmediato de Información (SII).

No obstante, esta Ley introduce nuevos requisitos que nos han llevado a mejorar diversos aspectos, para asegurar el máximo nivel de cumplimiento y en particular cabe citar todas las medidas para garantizar la trazabilidad de las operaciones realizadas y la inalterabilidad de los registros que afectan a esta trazabilidad, lo que aporta a LIBRA un nivel de control muy superior al que ofrecían las opciones de auditoría existentes hasta ahora. En este sentido, las mejoras introducidas van más allá de lo que exige la Ley, siendo un aspecto que consideramos que puede aportar un gran valor a las empresas en materia de auditoría y control interno.

Asimismo, EDISA ha llevado a cabo la formación del personal de la empresa para dar a conocer el alcance de esta Ley y también lo ha hecho con su base actual de clientes, para presentar todas las implicaciones que tiene la misma y también para establecer los aspectos cuyo cumplimiento corresponden directamente a los clientes.

## 2. Responsabilidades de la empresa usuaria LIBRA

A continuación, se detallan los aspectos que define la Ley, cuyo cumplimiento cae del lado de la empresa usuaria de LIBRA y que por tanto la empresa debe conocer y asumir la responsabilidad de dicho cumplimiento.

### 2.1 Uso de LIBRA acorde a lo establecido en la Ley

El cliente se compromete a hacer un uso responsable de LIBRA, de acuerdo a lo que establece la Ley. LIBRA por diseño, no dispone de ninguna opción que facilite que una empresa pueda defraudar. El cliente se compromete a informar a EDISA de cualquier fallo u opción que pueda existir que pudiera afectar al cumplimiento de la Ley.

Asimismo, el cliente se compromete a no desarrollar ningún tipo de personalización o a realizar la alteración de datos de forma externa al programa LIBRA, que puedan vulnerar la Ley.

LIBRA no permite la modificación o el borrado de datos siguiendo las directrices de la Ley y en cualquier caso, LIBRA dejará rastro de todas las operaciones realizadas, tanto las que se lleven a cabo desde los programas LIBRA, como las que se realicen de forma externa mediante acceso directo a la base de datos. No obstante, consideramos importante destacar esta cuestión, ya que EDISA no se podrá hacer responsable de una posible alteración de los datos en el caso de que el cliente pueda tener acceso directo a la base de datos, aunque LIBRA deje rastro de dicha alteración.

Asimismo, LIBRA incluye opciones de cierre de periodo, tal como especifica el reglamento en su apartado 8.2.b, pero es la empresa usuaria quien se responsabiliza del uso de estas opciones de cierre.

### 2.2 Política de copias de seguridad

El cliente será siempre responsable del mantenimiento de sus copias de seguridad, para lo que contará con el apoyo técnico de EDISA que se pueda requerir.

En concreto y a la vista de lo establecido en la Ley, el cliente se responsabilizará de implantar un sistema de copias seguras en base a unas políticas definidas que incluyen las buenas prácticas del sector, como son:

- Realizar copias de seguridad firmadas, con clave.
- Realizar copias de seguridad en dos ubicaciones geográficas separadas y en dos medios diferentes.
- Disponer de un log de acceso o posible modificación de las mismas.

La nueva Ley exige que la empresa usuaria de LIBRA pueda proporcionar a la agencia tributaria un sistema que muestre la situación a una determinada fecha, dentro de los periodos tributarios a los que esté obligado el cliente.

Este hecho obliga a conservar al menos una copia anual del entorno completo de LIBRA, correspondiente a los últimos años (normalmente últimos cinco años). Asimismo, la norma también establece unos requisitos de conservación de información, lo que nos lleva a recomendar el siguiente esquema que consideramos que cumple lo establecido en la Ley a la vez que aportará a la empresa un mayor nivel de seguridad;

<b>PERIODICIDAD</b>	<b>UBICACIÓN</b>	<b>CONTENIDO</b>	<b>NUMERO DE COPIAS RETENIDAS</b>
COPIA DIARIA	PROPIA EMPRESA O CLOUD	PROGRAMAS Y DATOS	6 (Una por día de la semana, copias incrementales)
COPIA DIARIA	SEGUNDA UBICACIÓN	PROGRAMAS Y DATOS	6 (Una por día de la semana, copias incrementales)
COPIA SEMANAL	PROPIA EMPRESA O CLOUD	PROGRAMAS Y DATOS	4 (Una completa, no incremental, del último día de la semana de las cuatro semanas del mes)
COPIA SEMANAL	SEGUNDA UBICACIÓN	PROGRAMAS Y DATOS	4 (Una completa, no incremental, del último día de la semana de las cuatro semanas del mes)
COPIA MENSUAL	PROPIA EMPRESA O CLOUD	MAQUINA COMPLETA	1 Último mes

COPIA MENSUAL	SEGUNDA UBICACIÓN	MAQUINA COMPLETA	1 Ultimo mes
COPIA ANUAL	SEGUNDA UBICACIÓN	MAQUINA COMPLETA	5 (Ejercicios fiscales)

Según este procedimiento, en el sistema en el que se encuentran los datos reales de la empresa (en los propios equipos del cliente o en Cloud), se retendrían las copias de la última semana de programas y datos a nivel incremental, las copias totales de cada semana del mes y una copia de la máquina completa del último mes. Esto debe tenerse presente de cara a dimensionar estos espacios de almacenamiento y a definir los procedimientos de copiado.

En el caso de instalaciones en Cloud, adicionalmente a esta política, se recomienda que el cliente disponga de un espacio de almacenamiento en sus propias instalaciones, con el fin de tener una copia de todos estos ficheros fuera de la nube, ya que EDISA no puede responsabilizarse de la integridad de los datos alojados en cualquier Cloud al ser una infraestructura sobre la que tengamos nosotros el control, actuando únicamente como intermediarios en su contratación.

Corresponde al cliente la responsabilidad de verificar periódicamente cualquiera de estas copias para verificar que el procedimiento de copiado es correcto y que la información puede recuperarse debidamente. Para ello el cliente contará con el apoyo de EDISA si se requiere por parte de éste.

Nota: Además de los programas y datos que afectan a la operativa diaria de LIBRA, es necesario prever el espacio que se puede requerir tanto on line, como off line para el almacenamiento de los ficheros de registro de cambios.

### **2.3 Políticas de actualización de sistemas**

Se debe asegurar que el software de sistema operativo, incluyendo otros como el sistema de motor de base de datos o las versiones de Web Logic y otros productos se actualizan periódicamente evitando vulnerabilidades que pudieran afectar a dimensiones como la conservación que nos marca la ley.

Asimismo, el cliente es responsable del cumplimiento de compatibilidad tecnológica definido por LIBRA, es decir de usar las versiones de producto compatibles o soportadas por LIBRA, incluyendo el propio cumplimiento de versiones soportadas por parte de LIBRA y por parte de ORACLE, tal como se define en el “acerca de...” accesible desde LIBRA.

El cliente es responsable de contar con los contratos de mantenimiento de software en vigor, que permitan realizar las actualizaciones descritas.

El cliente deberá informar a EDISA de cualquier vulnerabilidad que pueda detectar que pueda afectar a la seguridad en el uso de LIBRA.

## 2.4 Políticas de contraseñas

La política de contraseñas define los requisitos de las contraseñas.

Algunas recomendaciones:

1. Las contraseñas deben ser fuertes (al menos 8 caracteres, uso de minúsculas/mayúsculas/números/símbolos)
2. No usar la misma contraseña para más de un servicio o sistema.
3. Cambiar la contraseña al menos dos veces al año.
4. No usar variaciones de contraseñas antiguas (por ejemplo, añadiendo un número a una contraseña antigua)
5. Como es casi humanamente imposible recordar todas las contraseñas seguras diferentes, se recomienda el uso de administradores de contraseñas o utilizar una validación centralizada mediante LDAP.

## 2.5 Políticas de control de acceso

La política de control de acceso define reglas y principios sobre los cuales se configuran los derechos y restricciones de acceso.

La política es aplicable a todo el personal interno y externo.

1. El acceso se otorga en base al principio de necesidad de saber/necesidad de usar.
2. Según el rol de la persona, se otorga acceso a la información/activo.
3. El acceso es otorgado/revocado sobre la solicitud de la gerencia. El usuario puede solicitar el acceso por sí mismo, pero luego la solicitud debe ser aprobada primero por su gerente.
4. Los derechos de acceso también serán otorgados/revocados como parte del Proceso de incorporación de Recursos Humanos y del Proceso de cese de recursos humanos.
5. Debe usarse 2FA (Autenticación de dos factores) para sistemas con información sensible (Política de clasificación de la información) en todo aquel sistema que lo proporcione.
6. Las ID's de usuario no se pueden reutilizar para sistemas que contienen información confidencial o sensible.

Requerimientos para sistemas de contraseñas

1. Debe solicitarse al usuario que cambie la contraseña predeterminada en el primer inicio de sesión
2. Debe obligarse al usuario a emplear contraseñas de calidad (según la Política de contraseñas)

3. Debe evitarse la reutilización de las últimas tres contraseñas
4. Libra debe de estar expuesto a internet a través de un Proxy Inverso que proporcione SSL a todas las comunicaciones.

## **2.6 Política criptográfica**

Define cuándo, dónde y cómo se usa la criptografía en nuestra organización, y cómo se realiza la administración de claves. Por ejemplo para la firma digital de facturas y logs así como el cifrado de copias de seguridad. Algunos requisitos:

1. Duración máxima para la firma de certificados es 1 año
2. La duración máxima de los certificados SSL/TLS es 2 años
3. Todos los certificados deben tener una longitud de clave de al menos 2048 bits o superior.
4. Todos los certificados deben administrarse a través de la gestión de activos en Certificados

## **2.7 Política malware y antivirus**

El cliente final es responsable de disponer en sus sistemas informáticos de medidas que minimicen la posibilidad de entrada de virus o cualquier tipo de malware que pudiera afectar a dimensiones como la conservación o integridad de la información, tal y como nos marca la ley.

El cliente final se compromete a implantar controles de detección, prevención y recuperación para proteger contra malware, combinados con el conocimiento apropiado del usuario.

En concreto:

1. Instalar herramientas antivirus / antimalware (y asegurarse de que estén actualizadas)
2. Evitar que los usuarios instalen software libremente.
3. Controles de red para evitar la descarga o ejecución de malware.
4. Concienciación y formación proactiva a los usuarios en materia de malware.
5. Segregación en redes.

## **2.7 Continuidad de las operaciones y del negocio de la empresa**

La continuidad de las operaciones y del negocio de la empresa depende de la disponibilidad de LIBRA y de los datos de la empresa. El cliente es responsable de que todos los medios hardware, de comunicaciones y las copias de seguridad estén disponibles para asegurar esta continuidad. Aunque EDISA pueda proveer servicios relacionados con el hardware, las comunicaciones o las copias de seguridad, corresponde al cliente la responsabilidad final de asegurar la continuidad de sus operaciones, no pudiendo trasladar a EDISA los posibles daños de tipo directo o indirecto, derivados de la imposibilidad de usar LIBRA, por falta de acceso o por posible pérdida de datos.

El cliente final es responsable de disponer de un plan de contingencia que minimice el riesgo de parada o incluso de pérdida de datos, tanto en el caso de que LIBRA funcione sobre un hardware propio de la empresa, como en el caso de encontrarse en una instalación alojada en un datacenter o Cloud, contratado directamente por la empresa o contratado a través de EDISA.

Aunque EDISA actúe como intermediario en la contratación de los servicios de un datacenter o cloud, el cliente reconoce que EDISA no es el proveedor original de esos servicios de alquiler de hardware y que por tanto la seguridad y disponibilidad de estos equipos y comunicaciones no dependen de EDISA y por tanto ante una parada o falta de acceso al datacenter, EDISA no tendría ninguna capacidad de actuación y por tanto no podría hacerse responsable de las consecuencias de dicha parada o incluso de una posible pérdida de datos. Ante tal situación, los datacenter con los que trabajamos habitualmente establecen unas penalizaciones por incumplimiento de los SLA (acuerdos de nivel de servicio), que suelen suponer la reducción de un porcentaje de la cuota facturada en el mes que se ha producido el incumplimiento del SLA, lo que suele representar un importe muy pequeño en relación al problema que puede haber sufrido la empresa, sobre todo si ésta no cuenta con un plan de contingencia. EDISA no puede más que trasladar al cliente esos mismos SLA de los proveedores de datacenter-cloud, estableciendo en cualquier caso una indemnización máxima a la empresa cliente del importe de los últimos 6 meses facturados (salvo que en el contrato se haya especificado algo diferente) en concepto de los servicios de alquiler o suscripción mensual del datacenter-cloud en el caso de una situación extrema en la que el fallo producido en el datacenter pudiera suponer la pérdida continuidad de las operaciones durante más de dos días (es decir, que se perdiera el acceso completo a LIBRA) o la pérdida de datos. Si se llegase a producir una situación de este tipo muy poco probable, se cancelaría el contrato de servicios de datacenter, asumiendo el cliente la contratación directa de estos servicios o la adquisición de un hardware propio.

### 3. Declaración de haber sido informado de las responsabilidades de la empresa

Como fabricante de software tenemos un amplio compromiso para proporcionar herramientas informáticas y procedimientos seguros que reducen al máximo la posibilidad de uso fraudulento de nuestro software LIBRA.

Pese a esto los clientes y distribuidores adquieren la responsabilidad de no utilizar o realizar cualquier acción orientada al incumplimiento de la Ley 11/2021 en todo su contenido, así como cualquier modificación o desarrollo informático que pueda alterar las medidas de seguridad y cumplimiento de la ley.

D. \_\_\_\_\_ en representación de la empresa \_\_\_\_\_, con CIF: \_\_\_\_\_ cliente de EDISA, declaro haber leído el Documento de adhesión para el uso del software LIBRA en su versión X.X, estando de acuerdo en el conjunto de operaciones de seguridad y buenas prácticas de las que deberá responsabilizarse nuestra empresa, orientadas al cumplimiento de Artículo 201 bis, Ley 11/2021, resumidas en la siguiente tabla.

ASPECTO TRATADO	HEMOS SIDO INFORMADOS
Uso de LIBRA acorde a lo establecido por la Ley	X
Cumplimiento de la política de copias de seguridad	X
Política de actualización de sistemas	X
Políticas de contraseñas	X
Política de control de accesos	X
Política criptográfica	X
Política de Malware y Antivirus	X
Continuidad de las operaciones y del negocio	X

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_\_

Por la empresa: Firmado