Política de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo

Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo

VERSIÓN: 1.0| FECHA: 17- 07 - 2 0 25
CLASIFICACIÓN: RESERVADA | REFERENCIA: E S C O M E U P 1

- **Ficha técnica**

Título del documento: Política de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo
Estado: No revocado
Tipo de documento: Política
Área funcional responsable: Departamento de Legal & Compliance

- **Aviso**

Eupago – Instituição de Pagamento, Lda - Sucursal en España se rige por una política de seguimiento y mejora continua de sus políticas y procedimientos. Por tanto, la información contenida en esta Política está sujeta a actualización y es reservada el hacía Departamento de Legal & Compliance el derecho a realizar dicha actualización.

- **Historial de versiones/revisiones**

Versión	Fecha	Descripción	Autor
1.0	16-07-2025	Versión original de la Política	Departamento Legal y de Conformidad

- **Índice**

Alcance	4
Cumplimiento	5
Capítulo I - Deberes preventivos del Sujeto Obligado	6
A. Medidas de diligencia debida	6
A.1 Medidas de diligencia debida simplificada	7
A.2 Medidas de diligencia debida reforzada	8
B. Obligación de comunicación	10
B.1 SISTEMA AUTOMATIZADO DE DETECCIÓN Y ANÁLISIS DE OPERACIONES SOSPECHOSAS	11
B.2 . DECLARACIÓN MENSUAL OBLIGATORIA DE OPERACIONES	13
C. Deber de conservación	17
D. Protección de Datos Personales en el Ámbito de PBC-FT	18
E. Obligación de presentación de declaraciones semestrales	22
F. Deber de colaboración	24
G. Deber de secreto	26
H. Deber de formación	27
Capítulo II - Organismos de Control Interno	29
Capítulo III - Gestión de riesgos de BCFT	31
Capítulo IV - Canal Interno de Denuncias	56
Glosario	58

Introducción

La presente Política de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo (en adelante, "la Política") establece el marco normativo interno de Eupago – Instituição de Pagamento, Lda. – Sucursal en España en relación con el cumplimiento de las obligaciones previstas en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y su reglamento aprobado por Real Decreto 304/2014, de 5 de mayo.

Eupago reafirma su compromiso con los más altos estándares de integridad, legalidad y ética empresarial, adoptando medidas sólidas para evitar ser utilizada como vehículo para el blanqueo de capitales o la financiación de actividades terroristas.

Alcance

Esta Política es de obligado cumplimiento para:

Todo el personal de Eupago en España, incluyendo empleados, responsables de áreas, directivos y miembros del órgano de administración.

Terceros y colaboradores que intervengan en procesos relacionados con clientes, operaciones financieras o cumplimiento normativo.

La Política se aplica a todos los productos, servicios, operaciones, procesos internos y relaciones comerciales de Eupago en territorio español, con especial atención a:

- ➔ El proceso de admisión y conocimiento del cliente (KYC).
- ➔ La ejecución de operaciones ocasionales, complejas o de riesgo.
- ➔ La relación con corresponsales, agentes o intermediarios.

Descripción

Eupago ha desarrollado un Sistema de Control Interno y Comunicación para la prevención del blanqueo de capitales y de la financiación del terrorismo, estructurado de la siguiente manera:

- ➔ Aplicación de medidas de diligencia debida según el riesgo del cliente, del producto y del canal de distribución.

- ➔ Procesos sistematizados de identificación formal y verificación documental antes

de iniciar relaciones de negocio.

- ➔ Herramientas tecnológicas para el seguimiento y análisis de operaciones inusuales, fraccionadas o sospechosas.

- ➔ Mecanismos de evaluación del riesgo global del negocio, conforme al enfoque basado en riesgo (Risk-Based Approach).

- ➔ Procedimiento interno para la comunicación de operaciones sospechosas al SEPBLAC, garantizando la confidencialidad.

- ➔ Conservación de documentación e información por un plazo mínimo de 10 años, conforme al artículo 25 de la Ley.

- ➔ Programas de formación continua y sensibilización para el personal, adaptados a las funciones y niveles de exposición al riesgo.

- ➔ Revisión anual del sistema mediante informes de autoevaluación, y auditorías internas o externas cuando sea necesario.

- **Cumplimiento**

El cumplimiento de esta Política es responsabilidad de todos los integrantes de Eupago en España, sin excepción. Para garantizar su aplicación efectiva:

- ➔ Se ha designado un Representante ante el SEPBLAC, que actúa como interlocutor único con las autoridades supervisoras.

- ➔ El Responsable de Cumplimiento Normativo (RCN) vela por la ejecución, actualización y supervisión del sistema interno.

- ➔ El Órgano de Administración asume la responsabilidad última de la implantación y funcionamiento del sistema de prevención, aprobando las políticas, asignando recursos y supervisando su eficacia.

- ➔ Se implementan controles internos, revisiones periódicas y un canal de comunicación interno para gestionar dudas, incidencias o incumplimientos en materia de PBC-FT.

Política de Prevención del Blanqueo de Capitales y de la Financiación del Terrorismo

- **Capítulo I - Deberes preventivos del Sujeto Obligado**

Eupago – Instituição de Pagamento, Lda. – Sucursal en España, en su calidad de sujeto obligado conforme al artículo 2 de la Ley 10/2010, de 28 de abril, asume el deber de adoptar y aplicar medidas adecuadas para prevenir y dificultar la utilización de sus servicios para el blanqueo de capitales y la financiación del terrorismo.

Este deber comprende la implementación de procedimientos internos eficaces de identificación, análisis, gestión de riesgos, control operativo, comunicación y archivo de la información relativa a los clientes y a las operaciones que realicen.

A. Medidas de diligencia debida

De conformidad con los artículos 3 a 12 de la Ley 10/2010, Eupago Sucursal en España aplicará medidas de diligencia debida adaptadas al nivel de riesgo asociado al cliente, producto, geografía y transnacionalidad , incluyendo:

- Identificación formal del cliente y del titular real, si lo hay.
- Verificación documental, utilizando fuentes fiables e independientes.
- Recogida de información sobre el propósito y naturaleza de la relación de negocios.
- Seguimiento continuo de la actividad del cliente para detectar incoherencias o comportamientos inusuales.
- Aplicación de diligencia reforzada en los casos legalmente establecidos (personas con responsabilidad pública, países de riesgo, estructuras fiduciarias complejas, etc.).
- Posibilidad de aplicar diligencia simplificada únicamente si concurren condiciones expresamente previstas.

Todas estas medidas deben adoptarse antes de establecer la relación comercial o ejecutar operaciones ocasionales superiores a los umbrales legales.

Sobre este asunto, consulte a la *Política de Identificación y Aceptación de Clientes* que contiene todo el proceso desarrollado por la institución de para cumplir con este deber de identificación.

A.1 Medidas de diligencia debida simplificada

Las medidas simplificadas de diligencia debida se aplican cuando los productos, operaciones o clientes presentan un riesgo reducido de blanqueo de capitales o de financiación del terrorismo. Su utilización está sujeta a regulación específica y a una evaluación previa por parte del sujeto obligado.

Conforme lo previsto en el artículo 9 de la Ley 10/2010 y los artículos 16 a 23 del Real Decreto 304/2014, Eupago Sucursal en España podrá aplicar medidas simplificadas de diligencia debida en aquellos supuestos en los que, tras un análisis previo y documentado, se determine que el riesgo de blanqueo de capitales o financiación del terrorismo es bajo.

Supuestos en los que puede aplicarse la diligencia simplificada

Se podrá aplicar diligencia simplificada únicamente cuando se cumplan todas las siguientes condiciones:

- Que se trate de clientes, productos, servicios o relaciones que hayan sido previamente clasificados como de bajo riesgo, tras evaluación basada en los factores de riesgo del cliente, producto, canal y ámbito geográfico.
- Que no existan indicadores de operaciones sospechosas, estructuras complejas, beneficiarios ocultos o falta de transparencia en la actividad.
- Que no concurran circunstancias que obliguen a aplicar diligencia reforzada.

Ejemplos típicos previstos en la normativa:

- Entidades financieras o sujetos obligados establecidos en Estados miembros de la UE o en países terceros equivalentes, sometidos a requisitos similares de PBC-FT y supervisados.
- Organismos públicos nacionales o internacionales con bajo riesgo reputacional y estructuras de control transparentes.
- Productos financieros de bajo valor o función limitada, como ciertas tarjetas prepagadas, siempre que cumplan los límites legalmente establecidos.

Medidas que pueden ser simplificadas

Cuando se determine que procede aplicar diligencia simplificada, las siguientes medidas podrán ajustarse o reducirse:

- Identificación y verificación del cliente y del titular real: se podrá hacer tras el establecimiento de la relación, siempre que no se retrase innecesariamente.
- Obtención de información sobre la finalidad y naturaleza de la relación de negocio: podrá ser parcial o contextual si el riesgo es muy bajo.
- Frecuencia de las actualizaciones de la documentación y del seguimiento de las operaciones: podrá ser menos frecuente que en las relaciones de riesgo normal, aplicándose, en el caso de Eupago Sucursal en España, el plazo de 5 años conforme a lo establecido para las cuentas clasificadas como de bajo riesgo.

Documentación y supervisión interna

La decisión de aplicar medidas simplificadas deberá estar:

- Justificada documentalmente en el expediente del cliente.
- Autorizada o validada por el Responsable del Cumplimiento Normativo (RCN).
- Revisada periódicamente, ya que la clasificación de riesgo puede variar a lo largo del tiempo.

La aplicación inadecuada de medidas simplificadas podrá suponer una infracción grave o muy grave según lo dispuesto en el Título IV de la Ley 10/2010.

A.2 Medidas de diligencia debida reforzada

Las medidas reforzadas de diligencia debida están reguladas principalmente en los artículos 11 a 16 de la Ley 10/2010.

Deben aplicarse siempre que exista un mayor riesgo de blanqueo de capitales o financiación del terrorismo, en función del cliente, la operación, el canal de distribución o el ámbito geográfico.

Supuestos en los que puede aplicarse la diligencia reforzada

Los sujetos obligados deberán aplicar medidas reforzadas, entre otros, en los siguientes casos:

- Relaciones no presenciales (art. 12 Ley): Cuando la identidad del cliente no se compruebe mediante presencia física, salvo que se utilicen medios seguros como firma electrónica cualificada o transferencia desde cuenta abierta a su nombre en entidad sujeta a PBC/FT.

- Corresponsalía bancaria transfronteriza (art. 13 Ley): Requiere evaluación de la reputación, controles internos del banco corresponsal extranjero y autorización expresa de la alta dirección.

- Personas con responsabilidad pública (PRP) (art. 14 Ley): Requiere verificación reforzada de la identidad, del origen de los fondos y autorización expresa para establecer o continuar la relación de negocio. Se aplica tanto a PRPs extranjeras como nacionales (estas últimas, desde 2021).

- Productos, operaciones o tecnologías propensas al anonimato (art. 16 Ley): Incluye criptomonedas, tarjetas prepago no recargables, monederos electrónicos sin límites de uso, etc. Es obligatorio realizar una evaluación documentada del riesgo.

- Clientes o operaciones con países de alto riesgo (art. 11 y art. 13 Ley): Cuando intervienen jurisdicciones designadas por la Comisión Europea o el GAFI como de riesgo estratégico.

Medidas Concretas que Deben Aplicarse

Las medidas reforzadas pueden incluir, de forma acumulativa o individual según el caso:

- Identificación más estricta del cliente y del titular real;
- Obtención de información detallada sobre el origen de los fondos y del patrimonio;
- Seguimiento continuo intensificado de la relación de negocio;
- Aprobación expresa de la alta dirección antes del inicio de la relación comercial;
- Documentación y análisis adicionales sobre el propósito y naturaleza de la relación.

Procedimientos Internos y Supervisión

- La aplicación de estas medidas debe estar documentada en el expediente del cliente y ser revisada periódicamente (1 año).

- Se exige una evaluación del riesgo concreta y actualizada, incluyendo indicadores geográficos, sectoriales y transaccionales.

- Su incorrecta aplicación puede constituir infracción grave o muy grave, conforme al Título IV de la Ley 10/2010.

B. Obligación de comunicación

Eupago Sucursal en España debe comunicar sin dilación al SEPBLAC cualquier hecho u operación, incluso no ejecutada, que pueda estar relacionado con el blanqueo de capitales o la financiación del terrorismo (artículos 17 a 24 de la Ley 10/2010).

La comunicación se realiza a través del representante ante el SEPBLAC, previa documentación interna del análisis efectuado.

El SEPBLAC es el órgano competente para recibir:

- Las comunicaciones por indicio relativas a hechos u operaciones sospechosas, conforme al artículo 18 de la Ley 10/2010.

- Las notificaciones de imposibilidad de abstenerse de ejecutar una operación, en los términos del artículo 19.

La comunicación se efectuará a través de los medios establecidos por el SEPBLAC. Se utilizará el formulario oficial **F19-1**, que define la estructura y contenido obligatorio de las comunicaciones por indicio. Solo se utilizarán medios alternativos si están expresamente autorizados por el SEPBLAC.

Cuando la operación sospechosa aún no se haya ejecutado, Eupago Sucursal en España deberá abstenerse de realizarla hasta que el SEPBLAC se pronuncie, siempre que ello sea posible. Si, por motivos técnicos o legales, no fuera posible abstenerse, la comunicación deberá efectuarse inmediatamente después de la ejecución, incluyendo una justificación documentada de dicha imposibilidad.

Se garantiza la confidencialidad del procedimiento y la prohibición de revelar al cliente o a terceros la existencia o el contenido de la comunicación (prohibición de revelación).

La entidad no asume responsabilidad por las consecuencias de la comunicación, salvo dolo o negligencia grave.

COMUNICACIÓN DE OPERATIVA SOSPECHOSA POR INDICIO (F19-1)
(Artículo 18 de la Ley 10/2010)

Sujeto obligado	
Número de documento identificativo del sujeto obligado	
Nombre del representante	
Referencia de la comunicación	
Fecha de la comunicación	

Identificación de los intervinientes en las operaciones

Conocimiento de los intervinientes en las operaciones

Descripción de las operaciones

Indicios de blanqueo de capitales

Gestiones y comprobaciones realizadas

Documentación remitida (relación de documentos que se adjuntan)

El representante

NOTA: La comunicación por indicio deberá realizarse utilizando el modelo de comunicación de operación sospechosa por indicio F19-1, conforme a lo establecido por el SEPBLAC.

B.1 SISTEMA AUTOMATIZADO DE DETECCIÓN Y ANÁLISIS DE OPERACIONES SOSPECHOSAS

Eupago Sucursal en España dispone de un sistema de gestión integrado que incorpora una lógica de detección automatizada de operaciones potencialmente sospechosas, basada en reglas de riesgo previamente parametrizadas. Este sistema ha sido configurado para generar alertas internas cuando una operación presenta características atípicas o incompatibles con los perfiles de riesgo definidos.

Estas alertas son posteriormente analizadas de forma manual por el Área de Cumplimiento Normativo, que lleva a cabo una evaluación detallada antes de considerar, en su caso, la comunicación al SEPBLAC.

Parámetros para el análisis manual

En el análisis y tratamiento de las operaciones identificadas como sospechosas por el sistema de gestión integrado, los colaboradores responsables deben examinar los siguientes elementos:

1. Tipo de cliente involucrado - Se debe verificar la naturaleza jurídica del cliente

2. Deben analizarse los documentos disponibles que acrediten su actividad

3. Racional económico de la operación - Evaluar si el importe y la naturaleza de la operación resultan coherentes con la actividad profesional y el sector económico del cliente.

4. Historial transaccional del cliente - Analizar el comportamiento transaccional del cliente durante los tres meses anteriores a la operación, con el fin de detectar desviaciones respecto de su patrón habitual.

5. Frecuencia, complejidad e inusualidad de la operación - Determinar si la operación presenta un carácter anómalo, innecesariamente complejo o no alineado con el perfil del cliente.

6. Posible vinculación con escenarios de BC/FT - Verificar si la actividad desarrollada por el cliente está potencialmente vinculada a sectores o escenarios de alto riesgo en materia de blanqueo de capitales o financiación del terrorismo.

7. Ubicación geográfica del cliente - Evaluar el país donde está domiciliado el cliente y verificar si se encuentra incluido en las listas de jurisdicciones de alto riesgo.

8. País de destino de los fondos - Comprobar el país al que se transfieren los fondos, según la ficha del cliente, y si este se encuentra clasificado como jurisdicción de riesgo elevado en materia de BC/FT.

9. Índice de fraude asignado a la transacción - Considerar el porcentaje de riesgo de fraude atribuido a la transacción por el sistema de gestión integrado. Esta información está disponible en el apartado denominado “Transacción” dentro del expediente de la operación.

10. Medio de pago utilizado - Evaluar si el instrumento de pago empleado (transferencia, tarjeta, efectivo, etc.) es consistente con el perfil del cliente y si

aporta factores de riesgo adicionales.

De este modo, siempre que se identifica una operación sospechosa o un conjunto de operaciones con indicios de riesgo, estas son analizadas por el Departamento de Legal & Compliance, que evalúa si los hechos configuran una posible transacción fraudulenta o relacionada con el blanqueo de capitales o la financiación del terrorismo.

En caso afirmativo, y conforme al procedimiento interno aprobado, se deberá:

- Documentar el análisis efectuado, con base en los criterios técnicos establecidos;
- Clasificar el expediente como "operación sospechosa";
- Informar inmediatamente al Representante ante el SEPBLAC, quien será responsable de validar la decisión y proceder a la comunicación oficial al SEPBLAC, en su calidad de interlocutor autorizado ante dicha autoridad.

La comunicación se realizará:

- Mediante el formulario oficial F19-1, respetando los formatos y medios definidos por el SEPBLAC;
- En el plazo más breve posible, en cumplimiento del artículo 18 de la Ley 10/2010;
- Garantizando la prohibición de revelación, es decir, sin notificar al cliente ni a terceros la existencia de la comunicación.

En los casos en los que la operación aún no se haya ejecutado, Eupago Sucursal en España deberá abstenerse de realizarla, siempre que ello sea técnicamente viable. Si no lo fuera, la operación se comunicará de forma inmediata posterior a su ejecución, acompañada de una justificación documentada que motive la imposibilidad de abstención.

B.2 . DECLARACIÓN MENSUAL OBLIGATORIA DE OPERACIONES

De conformidad con el artículo 20 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, los sujetos obligados deben comunicar al SEPBLAC, con una periodicidad mensual, las operaciones que se establezcan reglamentariamente.

Esta disposición se desarrolla en el artículo 27 del Reglamento de la Ley, aprobado por el Real Decreto 304/2014, de 5 de mayo, el cual determina que, en todos los casos, los sujetos obligados deben comunicar mensualmente al SEPBLAC las siguientes operaciones:

Operaciones sujetas a comunicación mensual obligatoria

1. Movimientos físicos de efectivo o documentos al portador, incluyendo:

    - Moneda metálica, billetes, cheques de viaje, cheques u otros documentos al portador emitidos por entidades de crédito;
    - Por un importe superior a 30.000 euros o su equivalente en moneda extranjera;
    - Se exceptúan las operaciones abonadas o cargadas directamente en cuentas de clientes.
      (No aplicable a Eupago Sucursal en España, dado que no presta servicios de envío de dinero en efectivo)

2. Envíos de dinero conforme a la Ley 16/2009, de 13 de noviembre, de servicios de pago:

    - Operaciones que impliquen movimiento físico de efectivo o documentos al portador;
    - Por un importe superior a 1.500 euros o su equivalente.
      (No aplicable a Eupago Sucursal en España, dado que no presta servicios de envío de dinero en efectivo)

3. Operaciones con personas físicas o jurídicas residentes, o que actúen por cuenta de residentes, en territorios o países designados por Orden Ministerial:

    - Incluye también las transferencias de fondos desde o hacia dichos territorios,
    - Siempre que el importe sea superior a 30.000 euros o su equivalente.

4. Movimientos de medios de pago sujetos a declaración obligatoria, conforme al artículo 34 de la Ley 10/2010.

5. Información agregada sobre la actividad de envío de dinero, conforme al artículo 2 de la Ley 16/2009:

    - Desglosada por país de origen o destino,
    - Y por agente o centro de actividad.

6. Información agregada sobre transferencias internacionales realizadas por entidades de crédito:

- Desglosada por país de origen o destino.

7. Cualesquiera otras operaciones que puedan ser determinadas por Orden del Ministro de Economía y Competitividad.

Resumen Operacional Eupago Sucursal en España

Etapa	**Descripción**
1.	Instalación de la aplicación DMO v3.0 e importación de certificados (SEPBLAC + OCI)
2.	Creación de entidad comunicante y representante
3.	Preparación de la declaración: positiva, de movimientos, fraccionada o negativa
4.	Importación de operaciones mediante archivo XML (si aplica)
5.	Validación, corrección de errores y envío a través de la DMO
6.	Archivo de comprobantes, registros y ficheros enviados
7.	Actualización anual de certificados y del software

Nota: *Este documento describe los pasos fundamentales para el envío de las comunicaciones mensuales obligatorias al SEPBLAC utilizando la aplicación DMO v3.0, conforme lo establecido en la Ley 10/2010 y el Real Decreto 304/2014*

La Guía de Usuario de la Aplicación DMO v3.0 puede consultarse en el sitio oficial del SEPBLAC, a través del siguiente enlace: https://www.sepblac.es/wp-content/uploads/2018/06/guia_de_usuario.pdf

Procedimiento Interno de Eupago Sucursal en España para la Comunicación Sistemática de Operaciones al SEPBLAC

Eupago Sucursal en España lleva a cabo la comunicación sistemática de operaciones al SEPBLAC conforme a las obligaciones establecidas en la Ley 10/2010, utilizando la aplicación oficial DMO v3.0. Este proceso es ejecutado de forma coordinada por los equipos de Cumplimiento Normativo (Compliance), Tecnología y Operaciones, según las responsabilidades y flujos descritos a continuación.

Responsabilidad Institucional

El equipo de Cumplimiento Normativo (Compliance) es responsable de la supervisión integral del proceso, asegurando su conformidad con la normativa vigente y la correcta comunicación con las autoridades. Los equipos de Tecnologías de la Información proporcionan soporte en la generación técnica de los ficheros XML y en el mantenimiento de los sistemas relacionados.

Generación y Validación de Datos

El equipo de Tecnologías de la Información extrae mensualmente los datos de las operaciones sujetas a comunicación desde los sistemas internos, aplicando los criterios previamente definidos. Dichos datos se procesan y convierten al formato XML, conforme al esquema técnico establecido por el SEPBLAC.

Posteriormente, el equipo de Cumplimiento Normativo (Compliance)realiza una validación técnica y funcional de los ficheros, verificando:

- La coherencia con los requisitos legales y técnicos,
- La calidad de los datos declarados,
- La ausencia de errores estructurales en el XML.

En caso de inexistencia de operaciones sujetas a comunicación durante el período correspondiente, se genera una declaración negativa, la cual también es firmada electrónicamente y enviada a través de la aplicación DMO v3.0, conforme a las instrucciones del SEPBLAC. Esta acción asegura el cumplimiento formal del deber de comunicación incluso en ausencia de actividad reportable.

Envío de la Comunicación

Una vez validados, los ficheros son firmados digitalmente y enviados al

SEPBLAC a través de la aplicación DMO v3.0. Se genera un acuse de recibo, el cual se conserva conforme a las obligaciones de archivo y control interno.

El Responsable ante el SEPBLAC es el encargado de efectuar el envío oficial de las declaraciones mediante la aplicación DMO v3.0, firmándolas electrónicamente con los certificados autorizados y garantizando el cumplimiento de los plazos legales.

Ciclo Mensual de Ejecución

El procedimiento se realiza mensualmente, dentro del plazo legal estipulado. El cumplimiento del calendario de envío es supervisado por el equipo de de Cumplimiento Normativo (Compliance), que también se encarga de mantener actualizados los certificados digitales y la infraestructura técnica asociada.

C. Deber de conservación

(De conformidad con el artículo 25 de la Ley 10/2010, de 28 de abril)

Plazo de conservación:

La documentación que formalice el cumplimiento de las obligaciones establecidas en la Ley 10/2010 deberá conservarse durante un período de diez años.

A partir de los cinco años desde la finalización de la relación de negocios o de la operación ocasional, dicha documentación solo podrá ser accesible por:

- los órganos de control interno,
- las unidades técnicas de prevención, y
- los responsables de la defensa jurídica de la entidad.

Documentación específica a conservar:

A efectos de su uso en investigaciones sobre posibles casos de blanqueo de capitales o financiación del terrorismo por parte del SEPBLAC u otra autoridad competente, se conservará:

- Copia de los documentos exigibles en aplicación de las medidas de diligencia debida: durante 10 años desde el fin de la relación de negocios o ejecución de la operación.
- Original o copia con fuerza probatoria de los documentos que acrediten las operaciones, los intervinientes y la relación de negocio: durante 10 años desde la

ejecución de la operación o la finalización de la relación.

Formato y soporte del archivo:

Las copias de los documentos de identificación recogidos en el artículo 3.2 de la Ley deberán almacenarse en soportes ópticos, magnéticos o electrónicos que garanticen:

- la integridad de los datos,
- su lectura correcta,
- la imposibilidad de manipulación, y
  su adecuada conservación y localización.

Sistema de archivo:

El sistema de archivo deberá garantizar una gestión eficaz y la disponibilidad inmediata de la documentación:

- para fines de control interno, y
- para atender en tiempo y forma los requerimientos de las autoridades competentes.

Identificación electrónica conforme al Reglamento eIDAS:

Cuando la identificación del cliente se realice conforme al Reglamento (UE) n.º 910/2014 eIDAS (electronic IDentification, Authentication and trust Services), se deberá conservar también la información y los datos que acrediten dicha identificación por medios electrónicos.

D. Protección de Datos Personales en el Ámbito de PBC-FT

De conformidad con lo establecido en el artículo 32.1 de la Ley 10/2010, el tratamiento de datos personales realizado por Eupago Sucursal en España para dar cumplimiento a las obligaciones contenidas en el Capítulo III de dicha ley está amparado por:

- El artículo 8.1 de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales, y

- El artículo 6.1.c) del Reglamento (UE) 2016/679 (RGPD).

Por tanto, no será necesario el consentimiento del interesado ni para el tratamiento de los datos personales ni para las comunicaciones de datos previstas en dicho capítulo, incluyendo expresamente las referidas en el artículo 24.2 de la Ley 10/2010.

Exclusión del deber de información

En virtud del artículo 32.2 de la Ley 10/2010 y conforme al artículo 14.5 del RGPD:

- No resultará de aplicación la obligación de información al interesado prevista en el artículo 14 del RGPD en relación con los tratamientos señalados.

- Asimismo, conforme al artículo 23 del RGPD, no será procedente atender el ejercicio de los derechos establecidos en los artículos 15 a 22 del mismo Reglamento (acceso, rectificación, supresión, oposición, portabilidad, etc.).

En caso de que un interesado ejerciera alguno de estos derechos, Eupago Sucursal en España se limitará a informarle expresamente de lo dispuesto en este artículo, indicando que los tratamientos están excluidos del régimen general de derechos por imperativo legal.

Estas limitaciones también se aplicarán a los tratamientos realizados por el Servicio Ejecutivo de la Comisión (SEPBLAC) en el ejercicio de sus funciones legales.

Encargados y responsables del tratamiento

En cumplimiento de la Ley 10/2010, el tratamiento de datos personales por parte de Eupago Sucursal en España – Instituição de Pagamento, Lda., Sucursal en España, se realizará con responsabilidad directa, conforme a lo establecido por la normativa de protección de datos.

Eupago Sucursal en España actuará como responsable del tratamiento para las siguientes finalidades:

- Identificación y verificación de clientes y titulares reales;
- Aplicación de medidas de diligencia debida;
- Detección, análisis y comunicación de operaciones sospechosas;

- Conservación y archivo de documentación conforme a los plazos legales;

Estas actividades serán ejecutadas exclusivamente por los órganos internos designados, según el artículo 26 ter de la Ley 10/2010, incluyendo el Representante ante el SEPBLAC y el Responsable de Cumplimiento Normativo (RCN).

En caso de subcontratar servicios técnicos o analíticos (por ejemplo, verificación de identidad, outsourcing de cumplimiento o soluciones tecnológicas), los proveedores actuarán como encargados del tratamiento, formalizando dicha relación mediante contrato que:

- Limite estrictamente el acceso a los datos;
- Prohíba su uso para fines propios;
- Exija medidas de seguridad equivalentes o superiores a las de Eupago Sucursal en España.

Actualmente, Eupago Sucursal en España no forma parte de ningún órgano centralizado de prevención (art. 27 de la Ley 10/2010). Si en el futuro se adhiere a una estructura de este tipo (por exigencia legal o decisión empresarial), se evaluará su papel específico como responsable o encargado del tratamiento.

Evaluación de impacto en protección de datos

Eupago Sucursal en España realiza una **Evaluación de Impacto en Protección de Datos (EIPD)** sobre los tratamientos previstos en este ámbito con el fin de:

- Identificar riesgos asociados a la confidencialidad y seguridad de los datos personales;

- Adoptar medidas técnicas y organizativas reforzadas que aseguren:

    - Confidencialidad
    - Integridad
    - Disponibilidad
    - Trazabilidad de accesos y comunicaciones

El tratamiento de estos datos sólo podrá ser realizado por los órganos de control

interno autorizados por el artículo 26 de la Ley 10/2010, quedando prohibido su acceso por personal no autorizado.

Medidas reforzadas de seguridad

Los ficheros, sistemas y registros creados por Eupago Sucursal en España – Instituição de Pagamento, Lda. – Sucursal en España para dar cumplimiento a las obligaciones establecidas en el Capítulo III de la Ley 10/2010 estarán sometidos a un régimen reforzado de seguridad, tanto a nivel técnico como organizativo.

En particular, se adoptarán las siguientes medidas:

- Protección física y lógica avanzada de los sistemas que contengan datos personales, incluyendo cifrado, segmentación de entornos y almacenamiento seguro.

- Controles de acceso estrictos, mediante sistemas de autenticación individualizada, limitación por perfiles, y registro automático de:

    - Identidad del usuario,
    - Fecha y hora del acceso,
    - Motivo o justificación de la consulta,
    - Ámbitos de información accedida.

- Auditorías técnicas periódicas, dirigidas a verificar la eficacia de las medidas de seguridad, detectar posibles vulnerabilidades e implementar mejoras continuas.

- Revisión de logs y trazabilidad completa, que permita reconstruir cualquier acceso o modificación de datos personales relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo.

Estas medidas se aplicarán de forma proporcionada al nivel de riesgo de los tratamientos y estarán alineadas con los principios de confidencialidad, integridad, disponibilidad y resiliencia establecidos en el RGPD.

Para información complementaria sobre el tratamiento de datos personales, derechos de los interesados y medidas de protección aplicables, deberá consultarse la Política de Privacidad vigente de Eupago Sucursal en España.

E. Obligación de presentación de declaraciones semestrales

De acuerdo con el artículo 18 de la Ley 10/2010 y lo establecido por el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC), los sujetos obligados deberán presentar una declaración semestral relativa a las operaciones sospechosas de blanqueo de capitales o financiación del terrorismo.

En caso de no haberse detectado ninguna operación sospechosa durante el semestre correspondiente, el sujeto obligado deberá presentar una declaración negativa, confirmando expresamente dicha ausencia.

➔ Responsabilidad y órgano competente

La responsabilidad de la elaboración y presentación de la declaración negativa corresponde al Representante ante el SEPBLAC, en coordinación con la Unidad Técnica de Prevención o el Órgano de Control Interno (OCI), según proceda.

➔ Plazos para su presentación

Las declaraciones negativas se presentarán con carácter semestral, en los siguientes plazos:

Semestre	Periodo de referencia	Plazo límite para el envío de la declaración negativa
1.º semestre	1 de enero a 30 de junio	Hasta el 30 de septiembre del mismo año
2.º semestre	1 de julio a 31 de diciembre	Hasta el 31 de marzo del año siguiente

➔ Procedimiento de elaboración

El procedimiento interno para la elaboración de la declaración negativa semestral comprenderá las siguientes etapas:

a) **Revisión documental y operativa interna**

El OCI deberá revisar los registros de operaciones, alertas generadas por el sistema de monitoreo, y comunicaciones internas relevantes para verificar si hubo indicios razonables de operaciones sospechosas.

b) **Confirmación de inexistencia de comunicaciones**

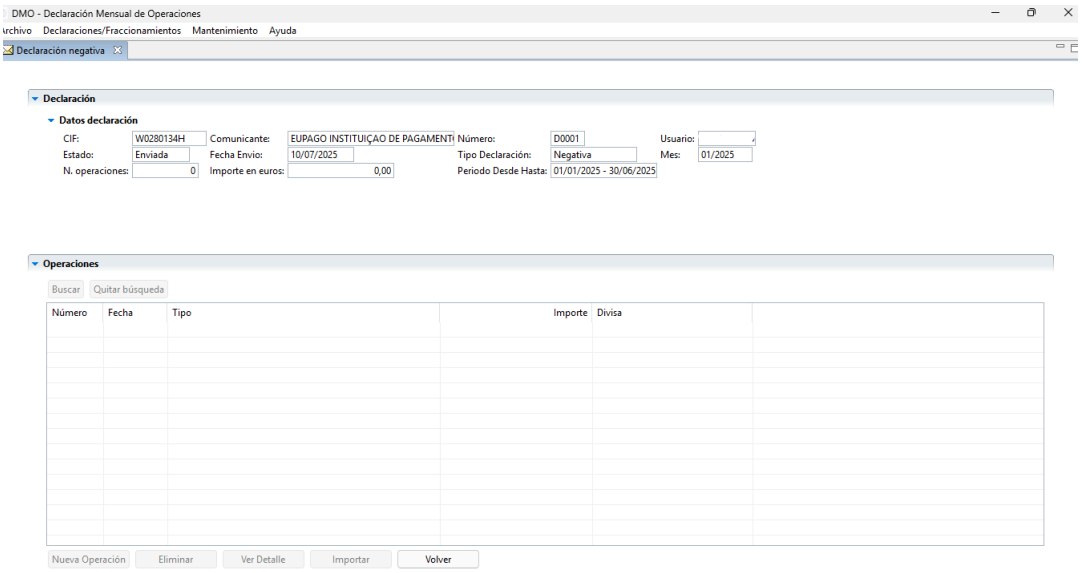
En caso de no haberse realizado ninguna comunicación por indicio al SEPBLAC durante el semestre, se certificará dicha inexistencia mediante acta interna.

c) **Redacción de la declaración negativa**

Se redactará la declaración negativa conforme al formato establecido por el SEPBLAC, incluyendo los datos identificativos del sujeto obligado y del representante.

d) **Firma electrónica y envío telemático**

La declaración será firmada electrónicamente por el Representante ante el SEPBLAC y enviada a través de la **Sede Electrónica del SEPBLAC**, mediante el sistema habilitado (e.g., formulario PDF firmado y certificado digital cualificado).



Nota: ***Ejemplo de declaración negativa enviada.***

➔ Incumplimiento o presentación fuera de plazo

El incumplimiento de esta obligación o la presentación fuera de los plazos establecidos podrá ser considerado una infracción leve o grave, conforme al régimen sancionador previsto en el Título IV de la Ley 10/2010.

F. Deber de colaboración

De conformidad con el artículo 21 de la Ley 10/2010, de 28 de abril, los sujetos obligados deben colaborar plenamente con la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (CPBCIM) y con sus órganos de apoyo, facilitando toda la información y documentación que les sea requerida en el ejercicio de sus competencias legales.

Esta obligación de colaboración es esencial para garantizar la eficacia del sistema de prevención y represión del blanqueo de capitales y de la financiación del terrorismo.

Obligación de Responder a los Requerimientos:

Eupago Sucursal en España-Instituição de Pagamento - Sucursal em España se compromete a:

- Facilitar, de forma completa y diligente, cualquier documentación o información solicitada por la CPBCIM o sus órganos de apoyo.

- Los requerimientos recibidos serán tratados con carácter prioritario y deberán ser atendidos dentro del plazo expresamente indicado en la solicitud.

- El requerimiento deberá especificar claramente:

    - La documentación concreta que debe aportarse o los extremos que deben informarse.
    - El plazo para su remisión.

En caso de que la documentación:

- No sea enviada dentro del plazo establecido, o
- Sea aportada de forma incompleta, omitiendo datos relevantes,

se considerará que no se ha cumplido con la obligación legal, pudiendo derivarse consecuencias sancionadoras.

Sistemas Internos de Respuesta

Para cumplir eficazmente con esta obligación, Eupago Sucursal en España-Instituição de Pagamento - Sucursal em España, implementa los siguientes mecanismos de control interno:

- Procedimientos definidos para la recepción, análisis y respuesta a comunicaciones de la CPBCIM u otras autoridades legalmente competentes.
- Sistemas informáticos estructurados que permitan verificar si se mantienen o se han mantenido relaciones de negocio con determinadas personas físicas o jurídicas.
- Identificación clara de la naturaleza de dichas relaciones, incluyendo el tipo de producto o servicio contratado y otras características relevantes.
- Designación de un responsable interno de interlocución con la CPBCIM, normalmente el Responsable de Cumplimiento Normativo (RCN), encargado de coordinar la recopilación de información y la respuesta correspondiente.

Responsabilidades Internas

El cumplimiento de esta obligación involucra a los siguientes actores internos:

- Responsable de Cumplimiento Normativo (RCN): recepción y análisis de los requerimientos, coordinación de la respuesta.

- Departamento de Cumplimiento (Compliance): apoyo en la recopilación de documentación, validación de la información y seguimiento de los plazos.

  Departamento de Sistemas y Tecnología: soporte en la obtención de datos y verificación técnica.

Todos los colaboradores deben garantizar la confidencialidad, integridad y disponibilidad de la información proporcionada a las autoridades.

Consecuencias del Incumplimiento

El incumplimiento de las obligaciones establecidas en este capítulo podrá dar lugar a:

- La apertura de un expediente sancionador por parte de la CPBCIM.
- La imposición de sanciones administrativas (multas, advertencias, etc.).
- La responsabilidad individual de los empleados que obstaculicen o retrasen injustificadamente el cumplimiento de los requerimientos.

Actualización y Formación

- Este capítulo será revisado periódicamente en función de los cambios normativos o interpretaciones regulatorias relevantes.

- Eupago Sucursal en España-Instituição de Pagamento - Sucursal en España garantiza la formación continua de sus empleados sobre los deberes de colaboración con las autoridades competentes, en especial en lo referente a los procedimientos descritos en este capítulo.

G. Deber de secreto

El deber de secreto establecido en el artículo 49 de la Ley 10/2010, de prevención del blanqueo de capitales y de la financiación del terrorismo, constituye una de las obligaciones fundamentales que deben cumplir los sujetos obligados. Su finalidad principal es garantizar la confidencialidad de la información obtenida o comunicada en el marco de las obligaciones legales en materia de prevención.

Sujetos obligados y ámbito de aplicación

El deber de secreto se aplica a:

- Sujetos obligados definidos en la ley (entidades financieras, notarios, abogados, promotores inmobiliarios, entre otros).

- Sus administradores, directivos, empleados y colaboradores, cualquiera que sea su vínculo contractual o función.

Estos están obligados a mantener en estricta confidencialidad toda la información relacionada con:

- Comunicaciones al SEPBLAC u otras autoridades competentes.

- Datos obtenidos en la aplicación de medidas de diligencia debida, monitoreo, análisis o comunicación de operaciones sospechosas.

Prohibición de divulgación

La información obtenida o comunicada no podrá:

- Ser utilizada para fines distintos a los establecidos en la ley.
- Ser revelada al cliente afectado ni a ningún tercero.

- Ser compartida de forma directa o indirecta fuera de los supuestos expresamente permitidos.

Excepciones al deber de secreto

El artículo 49 contempla determinadas excepciones en las que no se considera infracción del deber de secreto:

- Intercambio de información entre entidades del mismo grupo empresarial, siempre que estén situadas en Estados con normativa equivalente y apliquen políticas comunes de prevención.

- Colaboración entre sujetos obligados que pertenezcan a la misma categoría profesional, con finalidades estrictamente relacionadas con la prevención.

- Asistencia legal o auditoría externa que requiera acceso a dicha información.

- Requerimientos judiciales o de autoridades competentes.

Consecuencias del incumplimiento

La revelación indebida de información amparada por el deber de secreto puede conllevar:

- Responsabilidad administrativa, incluida la imposición de sanciones por infracción grave o muy grave.

- Consecuencias disciplinarias dentro de la organización.

- Responsabilidad penal, si concurre violación de secretos profesionales.

H. Deber de formación

Todos los sujetos obligados deben garantizar que sus empleados, directivos y administradores reciban formación adecuada y continuada en materia de prevención del blanqueo de capitales y de la financiación del terrorismo, tal y como establece el artículo 29 de la Ley 10/2010.

La formación debe permitir que el personal:

- Conozca las tipologías y señales de alerta asociadas al blanqueo de capitales y la financiación del terrorismo.
- Comprenda las obligaciones legales y reglamentarias aplicables a su función.
- Sepa aplicar los procedimientos internos de control y las medidas de diligencia debida.
- Esté capacitado para detectar operaciones sospechosas y actuar conforme a los protocolos establecidos.

La formación será obligatoria para:

- El órgano de administración y dirección.
- Los miembros del Órgano de Control Interno (OCI) y del área de cumplimiento.
- El Representante ante el SEPBLAC.
- Todo el personal con funciones comerciales, de gestión de clientes, control, auditoría o análisis de operaciones.
- El personal de nueva incorporación, que deberá ser formado de forma inmediata tras su entrada.

El programa formativo incluirá al menos:

- Fundamentos del blanqueo de capitales y la financiación del terrorismo.
- Marco legal: Ley 10/2010 y su desarrollo reglamentario.
- Obligaciones de diligencia debida, comunicación por indicio, conservación de documentos, etc.
- Estructura y funcionamiento del sistema interno de prevención.
- Tipologías de riesgo sectoriales.
- Casos prácticos, ejemplos reales y jurisprudencia relevante.
- Actualizaciones normativas y cambios regulatorios.

Plazo:

La formación deberá impartirse con carácter periódico, al menos una vez al año.

Se realizarán actualizaciones siempre que haya modificaciones legislativas, reglamentarias o cambios en los procedimientos internos de prevención.

El sujeto obligado conservará evidencia documental de cada acción formativa realizada, que incluirá:

- Planes de formación y materiales didácticos.
- Registro de participantes con nombre, cargo y firma.
- Certificados o constancia de realización.
- Evaluaciones (si proceden) y resultados.
- Informes de necesidades formativas y seguimiento.

El Órgano de Control Interno será responsable de:

- Identificar las necesidades formativas del personal.
- Elaborar el plan anual de formación.
- Verificar la correcta ejecución y documentación de las acciones formativas.
- Informar al órgano de administración y al Representante ante el SEPBLAC.

El incumplimiento de la obligación de formación, o su inadecuación respecto a los riesgos y funciones del personal, podrá ser considerado como infracción grave o muy grave, conforme al régimen sancionador previsto en la Ley 10/2010.

- **Capítulo II - Organismos de Control Interno**

Representante ante el SEPBLAC:

El representante ante el SEPBLAC es la persona física designada por el sujeto obligado como interlocutor con el Servicio Ejecutivo de la Comisión (SEPBLAC) y otras autoridades competentes, conforme al artículo 26.1 de la Ley 10/2010.

Funciones y responsabilidades:

- Actuar como interlocutor único de la entidad ante el SEPBLAC y otras autoridades de supervisión en materia de PBC-FT.

- Coordinar la comunicación de operaciones sospechosas, asegurando que las notificaciones cumplan los requisitos legales.

- Supervisar la aplicación efectiva del sistema de control interno en materia de PBC-FT.

- Garantizar la implementación de las políticas y procedimientos internos de prevención y detección de operaciones de riesgo.

- Aprobar y/o validar los informes periódicos de seguimiento y evaluación del sistema de PBC-FT.

- Elevar al órgano de administración propuestas de mejora y alertas de posibles deficiencias o incumplimientos.

- Promover la formación continua del personal en las obligaciones legales y riesgos asociados.

La designación del representante debe ser comunicada formalmente al SEPBLAC mediante el procedimiento establecido, y deberá recaer en una persona con experiencia, conocimientos y capacidad de decisión.

Órgano de Administración en materia de PBC-FT

El órgano de administración (consejo de administración, administrador único o equivalente) tiene la responsabilidad última sobre la aprobación e implementación de las políticas y medidas de prevención del blanqueo de capitales y de la financiación del terrorismo.

Funciones y responsabilidades:

- Aprobar la política general de PBC-FT y los procedimientos de control interno.

- Asegurar que se asignen recursos adecuados y suficientes para el cumplimiento normativo.

- Designar formalmente al representante ante el SEPBLAC y al responsable del cumplimiento normativo.

- Revisar y validar, al menos una vez al año, el informe de autoevaluación del sistema de prevención.

- Supervisar las revisiones internas o auditorías externas sobre el sistema de PBC-FT.

- Impulsar una cultura de cumplimiento a todos los niveles de la organización.
- Garantizar la independencia y autonomía del área de cumplimiento normativo.

Ambos roles —representante ante el SEPBLAC y órgano de administración— deben actuar de forma coordinada y documentada, garantizando la trazabilidad de las decisiones estratégicas y operativas en esta materia.

- **Capítulo III - Gestión de riesgos de BCFT**

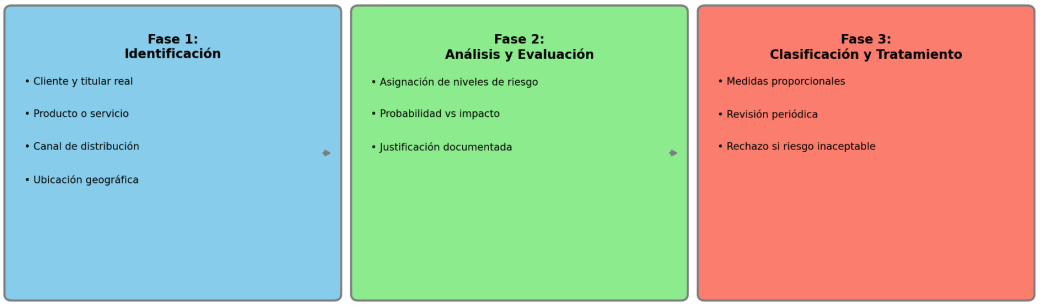
De conformidad con lo establecido en el artículo 32 de la Ley 10/2010, de 28 de abril, y los artículos 32 a 36 del Real Decreto 304/2014, Eupago Sucursal en España ha implementado un Sistema de Gestión del Riesgo de BC/FT basado en el enfoque basado en el riesgo (Risk-Based Approach). Este sistema permite identificar, evaluar y mitigar los riesgos inherentes al modelo de negocio, ajustando los controles y medidas de diligencia debida según el perfil de riesgo de los clientes, productos, canales y geografías implicadas.

La gestión del riesgo se desarrolla en tres fases principales:

1. Identificación de factores de riesgo inherentes: de cliente, producto/servicio, canal de distribución y ubicación geográfica;
2. Análisis y evaluación del nivel de riesgo: considerando probabilidad, impacto y consecuencias;
3. Clasificación y tratamiento: con aplicación proporcional de medidas simplificadas, estándar o reforzadas, según lo previsto en los artículos 9 a 11 de la Ley 10/2010.

Este proceso está documentado y se revisa al menos una vez al año o cuando se produzcan cambios relevantes en el modelo de negocio, de acuerdo con lo dispuesto en el artículo 35 del Real Decreto 304/2014.

El modelo actual se presenta de la siguiente manera:



A. Modelo de gestión de riesgos de BCFT

A.1. Identificación de los factores de riesgo de BC/FT (Fase 1)

De conformidad con el artículo 32 de la Ley 10/2010 y los artículos 32 a 34 del Real Decreto 304/2014, Eupago Sucursal en España realiza una identificación sistemática de los factores de riesgo inherentes asociados al blanqueo de capitales y financiación del terrorismo, en relación con los siguientes ejes:

1. Cliente y titular real;
2. Producto, servicio o transacción;
3. Canal de distribución o relación no presencial;
4. Área geográfica vinculada.

Estos factores se evalúan de forma individual y combinada, utilizando fuentes internas y externas, como listas de sanciones internacionales, publicaciones del GAFI (FATF) y directrices de la Autoridad Bancaria Europea (EBA/GL/2021/02).

La identificación de estos riesgos es responsabilidad del Departamento de Legal & Compliance, y se revisa periódicamente o ante cualquier cambio sustancial en el modelo de negocio.

FACTORES DE RIESGO INHERENTES AL CLIENTE:

De acuerdo con lo previsto en el artículo 33 del Real Decreto 304/2014, y en las Directrices EBA/GL/2021/02, Eupago Sucursal en España identifica los siguientes

factores de riesgo inherentes relacionados con el cliente o el titular real, que deben ser evaluados de forma individual y combinada:

1. **Tipo de cliente**

- Personas jurídicas con estructuras opacas o complejas

Constituyen un factor de riesgo relevante aquellas personas jurídicas cuya estructura de propiedad o control dificulte la identificación del titular real, o cuya configuración no se justifique con criterios económicos o funcionales legítimos.

Según el artículo 4 de la Ley 10/2010 y el artículo 8 del RD 304/2014, la identificación del titular real es obligatoria y debe ser completa y verificable. La opacidad en la estructura societaria eleva el riesgo de que la entidad sea utilizada para fines de blanqueo de capitales o encubrimiento patrimonial.

Ejemplos típicos:

- **Accionistas fiduciarios o testaferros**, especialmente cuando actúan por cuenta de terceros no identificados;
- **Acciones al portador** o instrumentos que dificulten la trazabilidad de la propiedad;
- **Entidades domiciliadas en jurisdicciones offshore**, sin presencia operativa real o sin relación económica aparente con el objeto social;
- **Estructuras societarias en cadena**, con múltiples niveles de sociedades interpuestas sin lógica comercial clara;
- **Clientes con frecuentes cambios de estructura accionarial o de domicilio social**, sin explicación económica coherente.

2. **Clientes ocasionales sin historial previo de relación**

La apertura de relaciones de negocio con clientes que no han mantenido vínculos previos con la entidad representa un riesgo adicional, al carecerse de referencias internas que permitan evaluar su comportamiento operativo, su perfil transaccional y su historial de cumplimiento.

Los riesgos asociados incluyen:

- Mayor probabilidad de uso instrumental de la entidad para fines ilícitos;

- Dificultad para detectar incoherencias, patrones atípicos o desviaciones, al no existir una base de comparación;
- Posible uso fraudulento de identidades o documentación falsificada durante el proceso de alta.

3. Clientes con alto nivel de rotación de cuentas o productos

La apertura y cierre frecuentes de cuentas, o la contratación sucesiva injustificada de productos distintos, puede ser indicio de una estrategia deliberada para evadir controles, disimular la titularidad real o encubrir operaciones sospechosas.

Los riesgos asociados comprenden:

- Fragmentación de la trazabilidad del comportamiento financiero del cliente;
- Simulación de actividad comercial legítima con fines de encubrimiento;
- Intento de eludir los mecanismos de detección automatizados y los controles internos.

FACTORES DE RIESGO INHERENTES A PRODUCTOS, SERVICIOS, TRANSACCIONES O CANALES DE DISTRIBUCIÓN:

En cumplimiento de los **artículos 32 y 33 del Real Decreto 304/2014**, y conforme a las **directrices emitidas por la Autoridad Bancaria Europea (EBA) (EBA/GL/2021/02)**, Eupago Sucursal en España identifica los siguientes factores como potencialmente elevados en términos de riesgo de blanqueo de capitales o financiación del terrorismo:

1. Productos o servicios con riesgo de opacidad o identificación limitada

Aunque Eupago Sucursal en España no ofrece productos con anonimato estructural, determinados elementos operativos asociados a la prestación de servicios de pago —especialmente en entornos digitales o no presenciales— pueden implicar un riesgo funcional de opacidad, dificultando la identificación efectiva del cliente o del titular real.

Estos escenarios pueden facilitar ocultar la identidad del titular real, suplantación de identidad mediante documentación falsificada o intento de utilizar los servicios de pago para canalizar fondos sin trazabilidad completa.

Factores de riesgo específicos:

- **Altas digitales sin presencia física del cliente**, donde el proceso de verificación de identidad depende de documentación escaneada o videoidentificación remota;
- **Operaciones iniciadas mediante plataformas o canales en línea**, donde no hay contacto directo con personal de la entidad;
- **Uso de representantes, intermediarios o estructuras societarias complejas**, sin justificación económica legítima o transparente;
- **Pagos o transferencias a terceros** que no guardan una relación clara con la actividad declarada por el cliente.

2. Contratación no presencial o mediante canales automatizados

En el contexto operativo de Eupago Sucursal en España, donde el alta y la contratación de servicios se realiza predominantemente a través de canales digitales, existen riesgos inherentes asociados a la **interacción remota**, especialmente si no se aplican controles técnicos reforzados o medidas de verificación sólidas.

Estos entornos, si no están adecuadamente controlados, pueden facilitar la suplantación de identidad mediante el uso de documentación alterada o robada, la falsificación de vínculos entre representantes y titulares reales, así como la admisión de clientes sin verificación efectiva del perfil económico y de riesgo.

Factores de riesgo específicos:

- **Altas realizadas exclusivamente por medios electrónicos**, sin verificación biométrica, videoidentificación u otros mecanismos equivalentes;
- **Uso de plataformas de terceros, APIs o marketplaces**, donde la captación y verificación inicial del cliente no depende directamente de la entidad;
- **Canales de distribución o intermediarios sin supervisión directa y continua**, que dificultan el control sobre la aplicación de medidas de diligencia debida.

3. Productos con alta rotación o volumen transaccional elevado

Ciertos servicios de pago, como la emisión de referencias o pagos instantáneos, pueden permitir una alta frecuencia operativa, especialmente en operaciones de pequeño valor, lo que puede dificultar la supervisión individualizada y favorecer el

fraccionamiento de movimientos económicos con origen dudoso.

Posibilita la dilución de la trazabilidad del origen de fondos, simulación de actividad económica legítima y evasión de controles mediante operaciones fragmentadas.

Factores de riesgo específicos:

- Servicios que permiten múltiples micropagos diarios o pagos fraccionados;
- Productos que no cuentan con límites automáticos por cliente, canal o transacción;
- Acceso masivo o abierto, sin segmentación de riesgo previa ni verificación documental rigurosa.

4. Servicios transfronterizos o con alcance internacional

Si bien Eupago Sucursal en España se centra principalmente en operaciones nacionales, la posibilidad de prestar servicios a clientes no residentes o realizar transferencias con componente internacional introduce un riesgo adicional cuando se vinculan jurisdicciones no cooperantes o sin supervisión equivalente.

Esto puede acarrear dificultad en la verificación del titular real, limitacion del alcance supervisor y posibilidad de canalización de fondos de origen ilícito.

Factores de riesgo específicos:

- Operaciones transfronterizas con jurisdicciones de alto riesgo (según GAFI, UE, SEPBLAC);
- Prestación de servicios a clientes domiciliados fuera del EEE, sin control suficiente del origen de fondos;
- Envío o recepción de pagos que no guarden relación clara con la actividad económica declarada.

5. Canales de distribución indirectos o externos

La contratación o promoción de servicios de pago a través de terceros, intermediarios o plataformas tecnológicas puede introducir un riesgo operativo si no existen mecanismos adecuados de control, supervisión y trazabilidad contractual.

Supone una pérdida de control directo sobre la admisión, seguimiento y revisión del cliente, limitando la capacidad de detectar a tiempo operaciones sospechosas o incumplimientos normativos.

Factores de riesgo específicos:

- Uso de intermediarios comerciales, agentes o APIs sin control directo por parte de Eupago Sucursal en España;

- Distribución delegada a entidades no sujetas a normativa equivalente de PBC/FT;
- Ausencia de contratos formales que regulen las obligaciones en materia de diligencia debida, protección de datos y supervisión del cliente final.

FACTORES DE RIESGO INHERENTES A LA UBICACIÓN GEOGRÁFICA:

La ubicación geográfica del cliente, del destinatario de los fondos o del país desde/hacia el cual se ejecutan operaciones puede constituir un factor de riesgo significativo en materia de prevención del blanqueo de capitales y financiación del terrorismo (BC/FT), especialmente cuando se vincula con jurisdicciones que presentan deficiencias estructurales, falta de cooperación internacional o elevada exposición a actividades delictivas.

Conforme a lo previsto en los artículos 32 y 33 del Real Decreto 304/2014, se considerarán de riesgo elevado aquellas relaciones o transacciones relacionadas con países o territorios que reúnan alguna de las siguientes características:

a) Deficiencias estratégicas en materia de PBC/FT, según listas oficiales del Grupo de Acción Financiera Internacional (GAFI/FATF) publicadas en www.fatf-gafi.org;
b) Inclusión en la lista de países terceros de alto riesgo de la Unión Europea, conforme al Reglamento Delegado (UE) 2016/1675 y actualizaciones posteriores: ver lista UE;
c) Jurisdicciones identificadas por fuentes creíbles (ej. informes del GAFI, FMI o Transparencia Internacional) como países con niveles significativos de corrupción u otra criminalidad sistémica;
d) Países o territorios sometidos a contramedidas financieras, embargos o sanciones internacionales, impuestas por el Consejo de Seguridad de las Naciones Unidas o la Unión Europea: ver sanciones ONU;
e) Jurisdicciones donde se detecta la presencia activa de organizaciones terroristas o desde las cuales se financian actividades terroristas;
f) Centros financieros offshore opacos o no cooperantes, con escasa regulación en materia de identificación del titular real;
g) Cualquier país o jurisdicción respecto de los cuales el SEPBLAC o el Órgano de Cumplimiento interno haya emitido directrices restrictivas basadas en criterios geográficos.

El Responsable de Cumplimiento Normativo deberá mantener actualizadas las fuentes de referencia y aplicar medidas reforzadas de diligencia debida en caso de identificar operaciones, relaciones comerciales u ocasionales asociadas a estos territorios.

A.2. Análisis de riesgos de BCFT (fase 2)

Una vez identificados los factores de riesgo inherentes (cliente, producto, canal, geografía), la segunda fase del sistema de gestión de riesgos de BC/FT consiste en analizar y valorar dichos riesgos con el objetivo de comprender su naturaleza, probabilidad de ocurrencia y consecuencias potenciales.

Este análisis permite establecer una clasificación relativa del riesgo y determinar qué medidas de mitigación deben aplicarse de forma proporcional.

El análisis tiene por objeto comprender por qué y cómo los actores criminales y terroristas utilizan los servicios financieros para ocultar, transformar o mover fondos ilícitos, identificar vulnerabilidades específicas del modelo operativo de Eupago Sucursal en España que puedan ser explotadas con fines delictivos así como evaluar el impacto potencial de dichos riesgos en la entidad, el sistema financiero y la sociedad.

El análisis de riesgos se basa en tres ejes:

1. Probabilidad de ocurrencia, o sea, una evaluación del grado de exposición de la entidad a cada tipo de riesgo, considerando su actividad, mercado, canales y perfil de clientes.
2. Impacto potencial, o sea, las consecuencias económicas, legales, operativas y reputacionales que podrían derivarse de una exposición no controlada al riesgo;
3. Clasificación del riesgo, o sea, una asignación de categorías: Bajo, Medio, alto o inaceptable, con base en matrices de riesgo y criterios definidos en el sistema interno.

El blanqueo de capitales busca ocultar el origen ilícito de fondos derivados de delitos como tráfico de drogas, corrupción, fraude fiscal o trata de personas. Por su modo, el financiamiento del terrorismo requiererecolectar, mover y distribuir fondos para mantener estructuras operativas o realizar atentados. Ambos fenómenos dependen del acceso a sistemas financieros legítimos pero vulnerables.

Aunque los efectos suelen analizarse a nivel nacional o global, también impactan directamente a nivel sectorial y empresarial:

- Pérdidas económicas para víctimas y ganancias ilícitas para delincuentes;
- Distorsión de flujos de capital y movimientos internacionales;
- Aumento artificial de precios en sectores sensibles;
- Competencia desleal frente a empresas legítimas;

- Daños a la reputación del sector financiero y pérdida de confianza;
- Riesgo de sanciones administrativas o penales;
- Contaminación de la economía formal con fondos ilícitos;
- Facilitación del terrorismo y de redes criminales organizadas.

El resultado del análisis deberá ser documentado formalmente, incluyendo la justificación de la calificación de riesgo, las medidas correctivas o preventivas adoptadas y el registro actualizado en el sistema de control interno.

Esta evaluación será revisada periódicamente o siempre que se detecten cambios relevantes en el entorno operativo, normativo o del cliente.

A.3. Evaluación de riesgos de BCFT (fase 3)

De conformidad con lo dispuesto en la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, y en su reglamento de desarrollo, el Real Decreto 304/2014, de 5 de mayo, Eupago Sucursal en España ha adoptado un enfoque basado en el riesgo (risk-based approach), tal como establece el artículo 3 de la Ley y las recomendaciones del Grupo de Acción Financiera Internacional (GAFI).

Una vez identificados y analizados los factores de riesgo inherentes (Fase 1), y evaluada su naturaleza, probabilidad de ocurrencia e impacto potencial (Fase 2), esta tercera fase tiene como objetivo llevar a cabo la evaluación final y clasificación del riesgo residual de BC/FT.

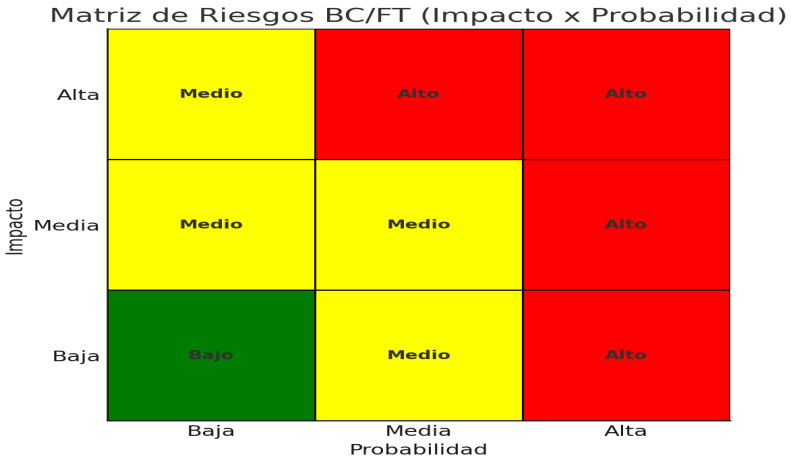
1. Matriz de Riesgos

Eupago Sucursal en España utiliza una matriz de riesgos como herramienta para evaluar y clasificar el riesgo residual de blanqueo de capitales y financiación del terrorismo (BC/FT), aplicando un enfoque basado en el riesgo conforme al artículo 3 de la Ley 10/2010 y al artículo 16 del Real Decreto 304/2014.

Este proceso permite asignar un nivel de riesgo global a cada cliente, producto, servicio, canal de distribución o jurisdicción, con base en una matriz de riesgos que combina dos ejes fundamentales:

- La probabilidad de ocurrencia del riesgo;
- El impacto potencial en caso de materialización

Cada factor evaluado se posiciona en la matriz y se clasifica de uno de los siguientes niveles de riesgo:



Cada factor evaluado se posiciona en la matriz y se clasifica dentro de uno de los siguientes **niveles de riesgo**:

- **Verde:**
  - **Riesgo bajo**: Riesgo aceptable. Se deben aplicar medidas estándar de diligencia debida.
- **Amarillo:**
  - **Riesgo Medio:** Riesgo moderado. Pueden requerir controles adicionales o medidas reforzadas.
- **Rojo:**
  - **Riesgo Alto:** Riesgo significativo. Se deben aplicar medidas reforzadas y se revisa la continuidad de relación.

El resultado de la evaluación determina la estrategia de gestión del riesgo, conforme a los artículos 11 a 16 de la Ley 10/2010. Asimismo, se establecerán las medidas internas de control, seguimiento y mitigación necesarias para gestionar adecuadamente dichos riesgos, de acuerdo con lo dispuesto en los artículos 26 y siguientes del Real Decreto 304/2014.

Este enfoque permite a Eupago Sucursal en España cumplir con su obligación de diseñar e implementar políticas, procedimientos y controles adecuados al perfil de riesgo de cada sujeto evaluado, conforme a los principios de proporcionalidad, eficacia y enfoque preventivo que exige la normativa vigente.

Toda evaluación debe estar debidamente documentada en el expediente correspondiente y quedar a disposición del Órgano de Control Interno y del SEPBLAC. El sistema deberá mantener un histórico actualizado de las evaluaciones realizadas.

EVALUACIÓN DE RIESGOS ASOCIADOS AL CLIENTE (PERFIL DE RIESGO DEL CLIENTE):

Eupago Sucursal en España lleva a cabo una evaluación sistemática del perfil de riesgo de cada cliente o comerciante, con base en criterios objetivos y conforme al principio de enfoque basado en el riesgo (Risk-Based Approach), de acuerdo con el Real Decreto 304/2014, artículo 33, y las Directrices EBA/GL/2021/02.

La evaluación considera los siguientes elementos:

1. **Naturaleza jurídica y estructura de propiedad:** Tipo societario, transparencia del titular real, existencia de estructuras complejas o fiduciarias.
2. **Actividad económica desarrollada:** Sector, volumen esperado de operaciones, vinculación con sectores de riesgo.
3. **Naturaleza, frecuencia y complejidad de las transacciones:** Volumen previsto, canales de pago utilizados, regularidad e inmediatez de los fondos.
4. **Historial y comportamiento previo del cliente:** Antigüedad de la relación, cumplimiento documental, alertas previas o incidencias operativas.

El perfil de riesgo del cliente se clasifica como **bajo** de forma automática si se verifica alguna de las siguientes situaciones:

- El cliente es una persona física o jurídica con actividad económica documentada, operativa en sectores sin riesgos específicos de BC/FT;
- Tiene residencia o sede en un país del EEE o equivalente, sin señales de alerta geográfica;
- La relación se establece a través de canales directos y controlados, con verificación presencial o digital completa;
- Cuenta con un historial de cumplimiento positivo, sin incidencias ni alertas.

Así el cliente clasificado con perfil de riesgo como bajo debe aplicar de forma obligatoria medidas estándar de diligencia debida, según el artículo 3 de la Ley 10/2010, revisión documental conforme al calendario general y seguimiento automatizado habitual, sin refuerzo adicional.

El perfil de riesgo del cliente se clasifica como medio si concurren elementos que, sin ser alarmantes por sí solos, requieren mayor vigilancia, tales como:

- Cliente de reciente incorporación o sin historial previo con Eupago Sucursal en España;

- ➢ Actividad económica legítima pero con algunos elementos de liquidez elevada o uso intensivo de efectivo;
- ➢ Estructura societaria sencilla pero con titular real no residente;
- ➢ Operaciones previstas en volumen o frecuencia ligeramente superiores a la media del segmento;
- ➢ Canal de alta digital no presencial sin videoidentificación.

Así el cliente clasificado con perfil de riesgo como medio debe aplicar de forma obligatoria medidas ampliadas o parciales de diligencia debida, revisión documental anual, monitorización proactiva de patrones de usos, con alertas automáticos configurados y evaluación de coherencia entre la actividad económica declarada y el comportamiento transaccional.

El perfil de riesgo del cliente se clasifica como alto de forma automática si se verifica alguna de las siguientes situaciones:

- Ubicación geográfica del cliente no justificada, con distancias significativas o incompatibles con la actividad económica declarada;
- Estructuras societarias opacas o complejas, sin justificación económica clara o con múltiples niveles interpuestos;
- Clientes cuya actividad esté vinculada a sectores con riesgo de corrupción o actividades delictivas (ej. tráfico de armas, apuestas ilegales);
- Clientes que tengan la condición de Persona Expuesta Políticamente (PEP), nacional o extranjera;
- Actividades en sectores de alta liquidez, como:
    - Juegos de azar;
    - Comercio de joyas, metales o piedras preciosas;
    - Venta de automóviles de lujo;
    - Turismo internacional intensivo;
    - Negocios que generen grandes cantidades de efectivo físico y dificulten la trazabilidad del origen de fondos.

Así el cliente clasificado con perfil de riesgo como alto debe aplicar de forma obligatoria medidas reforzadas de diligencia debida, según el artículo 11 de la Ley 10/2010, validación documental ampliada y revisión periódica con mayor frecuencia.

El perfil de riesgo del cliente se clasifica como inaceptable cuando el cliente o la operación

- Presenta indicadores de riesgo extremo no mitigables;
- Tiene origen en país sancionado, no cooperante o sometido a contramedidas del GAFI o la UE;

- Muestra incoherencias graves en la información proporcionada o rechazo a facilitar documentación clave;
- Se detecta actividad sospechosa no justificada y se presume uso instrumental de la entidad para fines ilícitos.

Así el cliente clasificado con perfil de riesgo como inaceptable debe hacer el rechazo inmediato de la relación o cancelación del alta, documentación del motivo y registro en el sistema de control interno y, en su caso, comunicación al SEPBLAC como operación sospechosa, según el artículo 18 de la Ley 10/2010.

EVALUACIÓN DEL RIESGO ASOCIADO AL PRODUCTO/SERVICIO O CANAL DE DISTRIBUCIÓN:

Eupago Sucursal en España evalúa el riesgo inherente vinculado a los productos y servicios ofrecidos, así como a los canales utilizados para su contratación o distribución. Este análisis tiene como finalidad identificar **posibles vulnerabilidades técnicas o operativas** que puedan facilitar el uso indebido de la entidad con fines de blanqueo de capitales o financiación del terrorismo.

Por defecto, los productos y servicios de Eupago Sucursal en España se consideran de **riesgo normal (moderado)**, salvo que exista evidencia (propia o proporcionada por autoridades competentes) que justifique una reclasificación como riesgo alto.

Producto/Servicio de riesgo **bajo**:

- ➢ Están disponibles exclusivamente para clientes identificados y verificados;
- ➢ No permiten el anonimato ni la transferencia entre titulares sin trazabilidad;
- ➢ No son susceptibles de ser utilizados como instrumentos de inversión, especulación o almacenamiento de valor;
- ➢ Se distribuyen a través de canales propios y controlados.

Producto/Servicio de riesgo **elevado:**

- ➢ Permiten una alta rotación transaccional o fraccionamiento operativo;
- ➢ Son accesibles mediante canales remotos no supervisados, APIs externas o plataformas de terceros;
- ➢ Pueden ser utilizados para transferencias internacionales, especialmente sin justificación económica clara;
- ➢ Están vinculados a operativas no presenciales con débiles mecanismos de autenticación;

- ➢ Son clasificados como sensibles por autoridades competentes (SEPBLAC, GAFI, EBA, etc.).

EVALUACIÓN DEL RIESGO ASOCIADO A LA UBICACIÓN GEOGRÁFICA:

La ubicación geográfica del cliente, del beneficiario o del país desde/hacia el cual se realizan operaciones constituye un factor relevante en la evaluación del riesgo de blanqueo de capitales y financiación del terrorismo (BC/FT), en cumplimiento del artículo 33 del Real Decreto 304/2014.

De esta forma, el perfil de riesgo se evalúa de la siguiente manera:

a) Si la ubicación geográfica es España, se considera riesgo "Bajo";

b) Si la ubicación geográfica está dentro de la UE (excepto España) se considera de riesgo "Normal";

c)Fuera de la Unión Europea consideramos que las ubicaciones geográficas tienen un nivel de riesgo "Alto".

Se consideran lugares considerados de riesgo inaceptable aquellos que:

a) Estén sujetos a sanciones internacionales, embargos o medidas restrictivas impuestas por el Consejo de Seguridad de las Naciones Unidas, la Unión Europea o el Consejo de Ministros de España;
b) Carezcan de marco legislativo eficaz de prevención del BC/FT;
c) Sean conocidos por apoyar directa o indirectamente el terrorismo;
d) Presenten niveles significativos de corrupción sistémica, criminalidad organizada o falta de cooperación internacional.

En estos casos, se prohíbe establecer relaciones de negocio y se documentará el rechazo correspondiente en el sistema interno.

Eupago Sucursal en España clasifica el riesgo geográfico con base en fuentes creíbles y actualizadas, tales como:

- GAFI / FATF: Listas de países de alto riesgo o bajo seguimiento → fatf-gafi.org
- Unión Europea: Lista de terceros países de alto riesgo → finance.ec.europa.eu
- Naciones Unidas: Sanciones internacionales → un.org/securitycouncil/sanctions
- Transparencia Internacional: Índice de percepción de corrupción → transparency.org
- SEPBLAC: Criterios adicionales y actualizaciones normativas → sepblac.es

CLASIFICACIÓN DEL GRADO DE RIESGO:

Una vez analizados los factores de riesgo relacionados con el cliente, el producto/servicio, el canal de distribución y la ubicación geográfica, Eupago Sucursal en España asigna a cada relación una clasificación global de riesgo, utilizando una metodología basada en la combinación de factores y el criterio de proporcionalidad.

Esta clasificación permite establecer qué medidas de diligencia debida deben aplicarse y con qué intensidad.

Los clientes pueden clasificarse según los siguientes niveles de riesgo:

a) **Bajo:** El cliente y sus operaciones no presentan señales de alerta, están plenamente identificados, operan en sectores económicos sin especial exposición y utilizan canales seguros y trazables.
b) **Normal:** Se detectan elementos con cierto riesgo potencial, aunque mitigados por otros factores (ej. actividad lícita, país de la UE, estructura societaria clara). Requiere control estándar con seguimiento reforzado en algunos casos.
c) **Alto**: Se identifican factores de riesgo significativos (ej. cliente PEP, jurisdicción no UE, producto sensible, estructura opaca). Se aplican obligatoriamente medidas reforzadas de diligencia debida conforme al Art. 11 de la Ley 10/2010.
d) **Inaceptable**: Existen riesgos críticos no mitigables (ej. país sancionado, imposibilidad de verificar el titular real, actividad claramente incoherente). No se establece relación de negocio ni se permite la operación.

Matriz de clasificación de riesgos	
	Factores de riesgo
Bajo	Los 3 factores se evaluaron como nivel de riesgo "**Bajo**".
Normal	1 Factor evaluado como "**Normal"** y 2 factores evaluados como **"Bajo"**. 2 Factores evaluados como **"Normal"** y 1 como **"Bajo".** Los 3 factores fueron evaluados como **"Normal"**.
Alto	Al menos 1 factor fue evaluado como con cierto grado de riesgo "**Alto"**
Inaceptable	Al menos 1 factor fue evaluado como con cierto grado de riesgo "**Inaceptable"**

ADECUACIÓN AL GRADO DE RIESGO:

Conforme al artículo 5 de la Ley 10/2010, las medidas de diligencia debida que deben aplicarse en cada caso deberán ser proporcionadas al nivel de riesgo asociado a la relación de negocio u operación ocasional, y ajustadas al resultado del análisis individual realizado.

Principios de adecuación:

1. **Clientes de riesgo bajo o normal:**
- Aplicación de medidas estándar de diligencia (artículo 3.º de la Ley 10/2010), incluyendo identificación, verificación y seguimiento general;
- Revisión documental conforme al ciclo de riesgo.

2. **Clientes de riesgo alto:**
- Aplicación obligatoria de medidas reforzadas de diligencia debida, según el artículo 11 de la Ley 10/2010;
- Verificación documental adicional, comprobación del origen de fondos, titularidad real, y autorización por el área de cumplimiento;
- Revisión periódica más frecuente

3. **Clientes de riesgo inaceptable:**
- No se permite la apertura de relaciones de negocio;
- En caso de detección de este nivel de riesgo en fase posterior, se procederá a la cancelación inmediata de la relación y posible comunicación al SEPBLAC.

B. Identificación y evaluación de riesgos específicos de BCFT en el contexto de la actividad

Conforme al enfoque basado en el riesgo previsto en el artículo 3 de la Ley 10/2010 y en el artículo 16 del Real Decreto 304/2014, Eupago Sucursal en España establece un sistema de análisis cualitativo y cuantitativo de los riesgos específicos asociados a su actividad, productos, servicios, clientes, canales y jurisdicciones.

Para ello, se emplea una metodología que combina la probabilidad de ocurrencia del riesgo con la gravedad de sus consecuencias en caso de materialización, conforme a la siguiente matriz de evaluación:

	Descargar (1)	**Promedio (2)**	**Alta (3)**
	Posibilidad de ocurrencia, pero con posibilidad de evitar el evento con el control	Posibilidad de ocurrencia, pero con posibilidades de evitar el evento	Fuerte posibilidad de ocurrencia y escasez de posibilidades de evitar el evento aún con

Probabilidad (PO)	existente para enfrentarlo.	mediante decisiones y acciones adicionales.	decisiones y añadidos esenciales.
Gravedad de la consecuencia (GC) **(Impacto financiero o reputacional)**	Daño a la optimización del desempeño organizacional, requiriendo la reprogramación de actividades o proyectos.	Pérdida en la gestión de operaciones, requiriendo redistribución de recursos en términos de tiempo y costos. Pérdida irrelevante de liquidez.	Daño a la imagen y reputación de la institución, así como a la eficacia y desempeño de su misión. Pérdida significativa de liquidez.

Una vez asignada la clasificación a cada una de las variables, se realiza la calificación final de riesgo en 3 niveles – Débil (1), Moderado (2) y Alto (3), de acuerdo a la siguiente matriz:

	Probabilidad de ocurrencia			
Gravedad y Consecuencia		**Descargar (1)**	**Promedio (2)**	**Alta (3)**
	Descargar (1)	**Débil (1)**	**Débil (1)**	**Moderado (2)**
	Promedio (2)	**Débil (1)**	**Moderado (2)**	**Alto (3)**
	Alta (3)	**Moderado (2)**	**Alto (3)**	**Alto (3)**

Una vez clasificados individualmente los riesgos específicos de cada dimensión evaluada (cliente, canal, producto, etc.) se calcula una media aritmética de las valoraciones obtenidas. Este promedio representa el nivel de riesgo final asignado al aspecto analizado.

Con base en esta calificación global, se determinan las medidas de diligencia debida, control interno y mitigación adecuada, en línea con los principios de proporcionalidad y enfoque preventivo exigidos por la normativa vigente.

B.1. Perfiles de riesgo del cliente

El Perfil de Riesgo del Cliente constituye uno de los elementos más relevantes y complejos dentro del modelo de prevención de blanqueo de capitales y financiación del terrorismo (BC/FT) de Eupago Sucursal en España. Su correcta determinación resulta esencial para garantizar una aplicación eficaz del enfoque basado en el riesgo, conforme a lo previsto en los artículos 3, 5, 11 y 16 de la Ley 10/2010, así como en las Directrices de la Autoridad Bancaria Europea (EBA) sobre gestión del riesgo de BC/FT.

Dado su carácter central en la evaluación general, la construcción y seguimiento del perfil de riesgo de cada cliente exige un análisis detallado y sistemático de múltiples factores, tanto individuales como combinados, incluyendo:

- Naturaleza jurídica y económica del cliente;
- Actividad profesional o empresarial;
- Jurisdicciones implicadas;
- Comportamiento transaccional;
- Canal de relación y medios utilizados;
- Nivel y tipo de diligencia debida aplicada.

El procedimiento completo para la evaluación del perfil de riesgo se detalla en el apartado específico “Evaluación de Riesgos Asociados al Cliente (Perfil de Riesgo del Cliente)”, que establece los criterios, metodologías y herramientas utilizadas por Eupago Sucursal en España para determinar el nivel de riesgo inherente y residual de cada cliente, así como las medidas de mitigación y seguimiento correspondientes.

B.2. Formas y medios de comunicación utilizados en el contacto con los clientes

En el contexto del modelo de prevención de BC/FT de Eupago Sucursal en España, las formas y medios de comunicación empleados en el establecimiento y mantenimiento de relaciones comerciales con los clientes constituyen un factor relevante de riesgo operativo y reputacional.

Los canales utilizados habitualmente incluyen Internet, el teléfono y el contacto presencial, siendo los dos primeros los más frecuentes en el modelo de negocio de la entidad. La utilización de medios no presenciales implica una mayor exposición a intentos de falsificación documental, suplantación de identidad de personas físicas o jurídicas, y mecanismos que buscan:

- Ocultar la identidad del titular real o del representante legal;
- Introducir fondos de origen ilícito en el sistema financiero;
- Eludir la fiscalidad o facilitar la fuga de capitales.

Con base en el análisis de escenarios de riesgo específicos, se ha elaborado la siguiente matriz de evaluación:

Formas y medios de comunicación utilizados en el contacto con los clientes				
Riesgo identificado	**Probabilidad de ocurrencia**	**Gravedad de Consecuencia**	**Grado de riesgo**	**Medidas Preventivas**
Una organización/individuo establece una relación comercial a distancia y envía copias de documentación falsificada.	Promedio (2)	Descargar (1)	Moderado (2)	Las copias y documentos necesarios para establecer una relación comercial sólo se aceptan si están autenticados o provienen de fuentes confiables.
Una organización criminal crea una sociedad limitada con una estructura compleja para "camuflar" al verdadero beneficiario.	Descargar (1)	Descargar (1)	Débil (1)	Una relación comercial sólo se establece si se conocen los propietarios beneficiarios de la empresa.
Una organización/individuo establece una relación comercial en persona y viene con copias de la documentación necesaria.	Promedio (2)	Descargar (1)	Moderado (2)	Las copias de los documentos siempre las realiza el empleado y utilizando los documentos originales.
Una organización criminal se hace pasar por propietaria de una empresa (ficticia) para justificar la emisión de referencias para recibir fondos ilícitos.	Promedio (2)	Descargar (1)	Moderado (2)	Solicitamos documentación a las empresas (por ejemplo, clave de acceso al certificado permanente) para validar los datos enviados por los potenciales clientes.
Un PEP/Titular de otro cargo político o público solicita la creación de una cuenta para un familiar directo, con el fin de poder recibir diversos pagos de sobornos y/o relacionados con actividades corruptas.	Descargar (1)	Descargar (1)	Débil (1)	Previo a establecer una relación comercial se realiza una búsqueda en el listado interno del individuo de PEPs/Titulares de otros cargos políticos o públicos, se realizan indagaciones y preguntas sobre la relación con PEPs/Titulares de otros cargos políticos o públicos o si ocupan cargos de la misma importancia.

Con base en las evaluaciones anteriores, se ha calculado una media aritmética del Grado de Riesgo de **1,6**, lo que posiciona el nivel de riesgo como **Moderado** para esta categoría.

En consecuencia, se aplicarán medidas de diligencia debida estándar con elementos reforzados en función de los indicadores de alerta presentes en cada situación, de acuerdo con los principios establecidos en los artículos 11 a 16 de la Ley 10/2010 y los artículos 26 y siguientes del Real Decreto 304/2014.

B.3. Naturaleza de las transacciones y productos y servicios prestados

Eupago Sucursal en España ofrece servicios de emisión y cobro de referencias Multibanco y Payshop, así como pagos a través de MBWay. Aunque estos métodos no son completamente anónimos, el uso de canales automáticos (por ejemplo, cajeros automáticos) elimina el contacto directo con empleados capacitados en la detección de operaciones sospechosas, lo que puede facilitar el uso indebido de estos servicios con fines ilícitos.

En este sentido, se han identificado posibles escenarios de riesgo derivados de la naturaleza de los productos y servicios, los cuales se evalúan mediante una combinación de probabilidad de ocurrencia y gravedad de la consecuencia, conforme al enfoque basado en el riesgo descrito en el artículo 3 de la Ley 10/2010 y el artículo 16 del Real Decreto 304/2014.

Naturaleza de las transacciones y productos y servicios prestados				
Riesgo identificado	**Probabilidad de ocurrencia**	**Gravedad de Consecuencia**	**Grado de riesgo**	**Medidas Preventivas**
Un grupo o individuo terrorista recluta personas para realizar pagos de bajo valor.	Descargar (1)	Descargar (1)	Débil (1)	Hay un sistema de alertas que analiza todas las transacciones en tiempo real, y es capaz de detectar transacciones realizadas de bajo valor.

Una empresa real, con actividad legal, y ya usuaria de nuestros servicios de pago, de repente aumenta drásticamente su facturación. Este incremento se debe a que se ha convertido en receptor de fondos de una Organización Criminal.	Descargar (1)	Descargar (1)	Débil (1)	La creación de herramientas analiza todas las cuentas mensualmente y calcula el monto promedio transaccionado por cliente. Si el promedio cambia significativamente en un mes, se envía un correo electrónico al gerente de Cumplimiento para que pueda analizar ese cliente en particular. El resultado de este análisis se entrega al Director General, se reduce a escrito y se archiva.

El análisis de los escenarios identificados arroja una media aritmética del Grado de Riesgo de **1**, lo que sitúa esta categoría en un nivel de **riesgo Débil.**

Así Eupago Sucursal en España dbe mantener medidas de control preventivo activo, incluyendo:

- Monitoreo automatizado de transacciones en tiempo real;
- Indicadores de alerta predefinidos;
- Revisión mensual de comportamiento transaccional
- Análisis documental y trazabilidad interna.

Estas acciones permiten mitigar el riesgo residual y cumplir con las exigencias establecidas en los artículos 5, 11 y 16 de la Ley 10/201, así como en el Real Decreto 304/2014 y las directrices de la EBA y del SEPBLAC en relación con la supervisión continua de productos, servicios y operaciones.

B.4. Naturaleza del área de negocio desarrollada

La actividad principal desarrollada por Eupago Sucursal en España se centra en la prestación de servicios de pago relacionados con la emisión y cobro de referencias Multibanco y Payshop, así como pagos mediante MB Way. Esta tipología de negocio, de alcance limitado y orientada al mercado nacional, no presenta una exposición significativa a riesgos elevados de blanqueo de capitales o financiación del terrorismo (BC/FT).

En consecuencia, y conforme al enfoque basado en el riesgo exigido por los artículos 3 y 5 de la Ley 10/2010, la naturaleza del área de negocio ha sido evaluada como de riesgo Débil.

Eupago Sucursal en España no desarrolla ninguna de las actividades tradicionalmente asociadas a un riesgo elevado de BC/FT, tales como:

- ➔ Servicios de banca corresponsal internacional que implican pagos comerciales a no clientes y servicios de banca privada internacional;
- ➔ Servicios de comercio y entrega de billetes de banco y metales preciosos;
- ➔ Servicios anónimos o fácilmente transferibles a través de fronteras, como banca en línea, tarjetas de valor almacenado, transferencias bancarias internacionales y empresas internacionales o fondos de inversión;
- ➔ Servicios de Crédito;
- ➔ Servicios de seguros;
- ➔ Servicios de Intercambio.

Por tanto, la exposición de Eupago Sucursal en España a amenazas derivadas del modelo de negocio es limitada y las medidas de control actuales resultan adecuadas y proporcionales al nível de riesgo identificado.

B.5. Naturaleza, dimensión y complejidad de la actividad de la Institución

La evaluación del riesgo de blanqueo de capitales y financiación del terrorismo (BC/FT) debe tener en cuenta el perfil estructural de la entidad obligada, incluyendo la naturaleza, la dimensión operativa y la complejidad de su actividad, conforme a lo previsto en el artículo 16 del Real Decreto 304/2014.

Se espera un volumen elevado de transacciones diarias, lo que impide el análisis individualizado por parte del personal. Para ello, se ha implementado un sistema de alertas en tiempo real, diseñado para detectar patrones irregulares o desviaciones sospechosas que pueden ser indicios de BCFT.

En cuanto la dimensión de la Institución, Eupago Sucursal en España cuenta con una plantilla reducida, pero todos los colaboradores con funciones comerciales y de decisión han recibido formación especializado en prevención de BCFT, impartida por el Instituto de Capacitación Bancaria. Así, en respecto a la dimensión de la Institución, el grado de riesgo se evalúa como Débil.

Además, la complejidad de la actividad de la Institución se considera Débil, por las siguientes razones:

a) El volumen de capital movido es bajo en comparación con otras actividades del sector financiero;
b) La institución no gestiona efectivo directamente, actuando como intermediario de pagos procesados por otras entidades supervisadas por el trata con dinero, sino únicamente con transacciones realizadas por otras instituciones sujetas a la supervisión del Banco de España.

Naturaleza, dimensión y complejidad de la actividad de la Institución				
Riesgo identificado	**Probabilidad de ocurrencia**	**Gravedad de Consecuencia**	**Grado de riesgo**	**Medidas Preventivas**
Un grupo o individuo terrorista recluta personas para realizar pagos fracionados de bajo valor.	Descargar (1)	Descargar (1)	Débil (1)	Sistema de alertas con análisis de transacciones en tiempo real, y detección de patrones anómalos..
Un grupo/individuo terrorista contacta empleados específicos que no no aplican los controles establecidos y se establece una relación comercial indebida.	Descargar (1)	Promedio (2)	Moderado (2)	El Departamento Legal & Compliance es responsable de aplicar los deberes normativos. Entre otros, se realiza una auditoria trimestral que revisa la correcta aplicación de los procedimientos en todas las cuentas abiertas desde la última revisión.

Del análisis realizado se obtiene una media aritmética de riesgo de **1,5**, por lo que se concluye que la naturaleza, tamaño y complejidad de la actividad de Eupago Sucursal en España implica un **riesgo Moderado**.

Este nivel de riesgo es gestionado mediante la aplicación de controles automatizados, protocolos de supervisión interna, y formación continua del personal, en línea con las obligaciones establecidas en la Ley 10/2010 y su normativa de desarrollo.

B.6. Canales de distribución de productos y servicios

El único canal de distribución (físico) en España es la oficina de la sucursal de Eupago Sucursal en España.

La mayoria de las relaciones comerciales se establecen a través de canales no presenciales, como Internet o por teléfono los cuales permiten el contacto y suscripción remota a los servicios ofrecidos.

Si bien estos canales amplían el alcance operativo, también incrementan ciertos riesgos operativos y de suplantación de identidad, propios de relaciones comerciales no presenciales.

Por ello, se han identificado y evaluado los siguientes escenarios de riesgo:

Canales de distribución de productos y servicios				
Riesgo identificado	**Probabilidad de ocurrencia**	**Gravedad de Consecuencia**	**Grado de riesgo**	**Medidas Preventivas**
Una organización/individuo establece una relación comercial a distancia y envía copias de documentación falsificada.	Promedio (2)	Descargar (1)	Moderado (2)	Las copias y documentos necesarios para establecer una relación comercial sólo se aceptan si están autenticados o provienen de fuentes confiables.
Una organización criminal crea una sociedad limitada con estructura compleja para ocultar al titular real	Descargar (1)	Descargar (1)	Débil (1)	Una relación comercial sólo se establece si se identifican claramente los titulares reales.
Una relación comercial se establece en persona, con presentación de copias de documentación.	Promedio (2)	Descargar (1)	Moderado (2)	Las copias se realizan exclusivamente por el personal, a partir de los documentos originales presentados.
Una organización criminal simula ser propietaria de una empresa ficticia para justificar ingresos de origen ilícito.	Promedio (2)	Descargar (1)	Moderado (2)	Se exige documentación adicional (por ejemplo, clave de acceso al certificado permanente) para verificar la veracidad de los datos suministrados.

La media aritmética del Grado de Riesgo para esta categoría es de **1,75**, por lo que se clasifica el nivel de **riesgo como Moderado** en lo relativo a los canales de distribución.

Como respuesta a esta evaluación, Eupago Sucursal en España aplica medidas de verificación reforzada en todas las relaciones no presenciales, garantizando el cumplimiento de los deberes de identificación y conocimiento del cliente (KYC) previstos en los artículos 6 a 12 de la Ley 10/2010 y en el Real Decreto 304/2014.

B.7. Grados de riesgo asociados a los países y áreas geográficas donde opera la Institución

De conformidad con lo dispuesto en los artículos 3, 11 y 16 de la Ley 10/2010 y en el artículo 24 del Real Decreto 304/2014, Eupago Sucursal en España identifica y evalúa el riesgo asociado a las jurisdicciones geográficas en las que residen o actúan sus clientes, así como los países vinculados a la operativa transaccional.

Actualmente, la sucursal de Eupago Sucursal en España en España presta servicios que tecnológicamente dependen de métodos de pago disponibles en Portugal, como la emisión y cobro de referencias Multibanco, Payshop y pagos a través de MB Way. En este contexto, la mayoría de los clientes (personas físicas o jurídicas) residen y operan en Portugal, país considerado como jurisdicción cooperante según los estándares del Grupo de Acción Financiera Internacional (GAFI) y el anexo de países de alto riesgo publicado por el SEPBLAC.

Para evitar riesgos derivados de jurisdicciones no confiables, Eupago Sucursal en España ha implantado controles automáticos que:

- Impiden el alta o mantenimiento de cuentas cuando el cliente o potencial cliente tiene residencia o dirección de contacto en un país clasificado como no cooperante o de alto riesgo;
- Activa alertas automáticas al responsable de Cumplimiento Normativo, de modo que pueda valorar la aplicación de medidas reforzadas o la denegación de la relación comercial.

Así, la exposición de Eupago Sucursal en España a riesgos derivados de jurisdicciones extranjeras es muy limitada, atento que:

- Los servicios ofrecidos no permiten anonimato no transferencias internacionales dura del marco SEPA;
- Todos los pagos son procesados a través de entidades supervisadas por el Banco de España o por autoridades homólogas del Espacio Económico Europeo;
- Se aplican medidas técnicas, organizativas y automatizadas para la detección de operaciones atípicas y el reporte inmediato de operaciones sospechosas al SEPBLAC, conforme a lo dispuesto en el artículo 18 de la Ley 10/2010.

Grados de riesgo asociados a los países y áreas geográficas donde opera la Institución				
Riesgo identificado	**Probabilidad de ocurrencia**	**Gravedad de Consecuencia**	**Grado de riesgo**	**Medidas Preventivas**
Un individuo "Front Man", a través de múltiples pagos de referencia, envía fondos a un PEP/Titulares de otros cargos políticos o públicos, quien, a través de la apertura de una empresa "legal", brinda la actividad de prestador de servicios/consultor.	Descargar (1)	Descargar (1)	Débil (1)	Hay un sistema de alertas que analiza todas las transacciones en tiempo real, y es capaz de detectar transacciones realizadas de bajo valor. Las cuentas de PEP/Titulares de otros cargos políticos o públicos están sujetas al cumplimiento del Deber de Diligencia Reforzado.

La evaluación resultante del promedio de los niveles de riesgo es 1, por lo que consideramos que respecto a los niveles de riesgo asociados a los países y áreas geográficas donde opera la Institución, existe un riesgo: **Débil.**

- **Capítulo IV - Canal Interno de Denuncias**

Este capítulo tem por objeto regular o funcionamento e as garantias do Canal Interno de Denuncias, implementado pela Eupago Sucursal en España Instituição de Pagamento, como medida de reforço do sistema de controlo interno em matéria de prevención del blanqueo de capitales y de la financiación del terrorismo, conforme estabelecido no artículo 26 bis de la Ley 10/2010, de 28 de abril.

Finalidad del Canal

El canal tiene como finalidad facilitar a empleados, directivos, relacionados un medio seguro, confidencial y accesible para comunicar hechos o conductas presuntamente irregulares, que pudieran constituir infracciones graves o muy graves, especialmente en relación con:

- Normas de prevención de blanqueo de capitales y financiación del terrorismo;
- Conductas contrarias al Código Ético o de Conducta de la entidad;
- Prácticas corruptas, fraudulentas o de gestión desleal.

Características del Canal

El canal de denuncias cuenta con las siguientes garantías:

- Acceso permanente y sencillo, a través de una funcionalidad integrada en la aplicación interna, accesible para todos los miembros de la entidad, el cual cumple con los requisitos exigidos para un canal de denuncias: está cifrado de extremo a extremo, todos los mensajes recibidos son anónimos y permite establecer comunicación de respuesta mediante un sistema de reenvío seguro y anonimizado y es accesible únicamente por el responsable del tratamiento.
- Posibilidad de realizar denuncias anónimas, sin perjuicio del seguimiento de la información.
- Confidencialidad absoluta sobre la identidad del denunciante y de los implicados.
- Protección frente a represalias para los denunciantes de buena fe.
- Limitación de acceso a las denuncias recibidas, exclusivamente a la persona específicamente designada para la gestión del canal, garantizando su independencia, confidencialidad y la ausencia de conflictos de interés.

Gestión de las Denuncias

Las denuncias recibidas a través del canal serán gestionadas mediante un procedimiento estructurado, que incluye:

- Registro.
- Asignación de una referencia al crear la denuncia. Esta referencia permitirá al denunciante acceder a ella y conocer su estado.
- Análisis preliminar y valoración de la verosimilitud.
- Investigación interna, si procede.
- Resolución y adopción de medidas correctoras o disciplinarias.
- Comunicación a autoridades competentes, en caso necesario.

Cumplimiento Normativo y Protección de Datos

El tratamiento de las denuncias se ajusta al Reglamento (UE) 2016/679 (RGPD) y a la Ley Orgánica 3/2018, asegurando que:

- Solo se conserven los datos estrictamente necesarios;
- Se eliminen aquellos que no sean pertinentes de forma inmediata;
- Se permita al denunciante ejercer sus derechos, cuando corresponda.

- **Glosario**

A los efectos de esta Política, se aplicarán las siguientes definiciones:

Riesgo - Probabilidad de que una operación, cliente, producto o canal contribuya al blanqueo de capitales o financiación del terrorismo.

Diligencia debida - Obligación de identificar y verificar la identidad del cliente, el propósito de la relación de negocios y el control continuo de la relación.

Beneficiario efectivo - Persona física que, en última instancia, posee o controla al cliente o en cuyo nombre se realiza una transacción.

Sujeto obligado - Persona física o jurídica sujeta a la Ley 10/2010, que debe implementar medidas de prevención del BC/FT.

Transacción - Cualquier operación económica, financiera o comercial susceptible de revisión en el marco del sistema de control interno.

Monitorización - Proceso continuo de supervisión de la actividad del cliente y detección de patrones inusuales.

Sucursal - Establecimiento permanente de una entidad extranjera que opera en España, sometido a la legislación española.

Entidad - Persona jurídica que presta servicios financieros o comerciales, incluida Eupago como institución de pago.

Medidas reforzadas - Controles adicionales aplicables en casos de mayor riesgo, como clientes PEP o jurisdicciones de alto riesgo.

Ley 10/2010 - Normativa española sobre prevención del blanqueo de capitales y financiación del terrorismo.

Real Decreto 304/2014 - Reglamento de desarrollo de la Ley 10/2010, que detalla las obligaciones de los sujetos obligados.

Blanqueo de capitales - Conversión o transferencia de bienes sabiendo que proceden de actividades delictivas para ocultar su origen.

Financiación del terrorismo - Provisión o recogida de fondos con la intención de ser utilizados en actividades terroristas.

Operación sospechosa - Transacción que, por su naturaleza, magnitud o complejidad, puede estar relacionada con BC/FT.

Comunicación por indicio - Obligación de reportar operaciones sospechosas al SEPBLAC según lo dispuesto en el artículo 18 de la Ley 10/2010.

Control interno - Sistema de políticas, procedimientos y herramientas destinados a prevenir riesgos de BC/FT.

Cliente - Persona física o jurídica que mantiene una relación comercial con la entidad.

Jurisdicción - País o territorio bajo un régimen normativo determinado. Puede influir en la clasificación de riesgo.

Alto riesgo - Clasificación que indica mayor probabilidad de exposición a BC/FT. Requiere medidas reforzadas.

Riesgo moderado - Nivel intermedio de riesgo que requiere revisión y seguimiento adicionales.

Riesgo bajo - Situación de riesgo reducido, que permite aplicar medidas simplificadas de diligencia debida.

Compliance- Función organizativa encargada de asegurar el cumplimiento normativo.

Institución de pago - Entidad autorizada para prestar servicios de pago conforme a la legislación europea.

Transparencia - Principio que exige que los clientes sean informados clara y completamente sobre el uso de sus datos.

Banco de España - Autoridad supervisora nacional para entidades de crédito y pago en territorio español.

Formación - Acción de capacitar a empleados sobre la normativa y los riesgos asociados al BC/FT.

Perfil transaccional - Conjunto de características habituales del comportamiento financiero de un cliente.Beneficiario: La persona física o jurídica que sea el destinatario previsto de los fondos que fueron objeto de una Transacción de Pago;

- **Lista de acrónimos y abreviaturas**

Para facilitar su explicación y sin perjuicio del eventual uso de denominaciones y expresiones que pretendan sustituir, a lo largo de la presente Política se utilizan las siguientes siglas y abreviaturas:

- **BCFT:** Blanqueo de capitales y financiación del terrorismo;

- **GAFI:** Grupo Grupo de Acción Financiera Internacional

- **EPI o PEP**: Persona expuesta políticamente;

- **EBA (European Banking Authority)**- Autoridad Bancaria Europea, emisora de directrices en materia de riesgos de BC/FT;

- **GDPR / RGPD** - Reglamento General de Protección de Datos (UE 2016/679) aplicable en toda la Unión Europea.

- **SEPBLAC** - Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias. Unidad de inteligencia financiera en España.

- **PEP (Persona con Responsabilidad Pública)** - Persona que desempeña o ha desempeñado funciones públicas relevantes, y cuyo perfil implica riesgo incrementado de BC/FT.