

Ingeniería de la Ciberseguridad  
Curso 2023/2024



# Práctica 1

## Sesión práctica 5:

PIA.

---

## Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

# ÍNDICE

<b>ÍNDICE</b>	<b>2</b>
<b>1. Descripción del tratamiento</b>	<b>3</b>
1.1. Propósito	3
1.2. Naturaleza	3
1.3 Ámbito/Alcance	4
1.4 Contexto	4
<b>2. Flujos de datos</b>	<b>4</b>
<b>3. Análisis de riesgos que afectan a la privacidad</b>	<b>7</b>
3.1 RIESGO DE TRATAMIENTO EXCESIVO	8
3.2 RIESGO DISCRIMINACION POR LA SITUACIÓN ECONÓMICA	8
3.3 RIESGO DE FALTA DE TRANSPARENCIA Y ACCESO A LOS DATOS	9
3.4 USO DE TERCEROS PROVEEDORES	9
3.5 TRANSFERENCIAS INTERNACIONALES DE DATOS	10
<b>4. Mapa de riesgos</b>	<b>11</b>

# 1. Descripción del tratamiento

## 1.1. Propósito

- **Fines últimos:** El fin último de ChaseMyCash es brindar a sus usuarios una herramienta tecnológica para administrar sus finanzas personales, permitiéndoles supervisar sus gastos, evaluar su situación financiera y tomar decisiones informadas para mejorar su bienestar financiero.
- **Fines instrumentales:** Los objetivos prácticos de la empresa incluyen el desarrollo y mantenimiento de la aplicación y sus servicios asociados, la adquisición y retención de clientes, la mejora continua del producto y la viabilidad económica.
- **Fines secundarios:** Entre las metas adicionales de la empresa se encuentran la generación de empleo y el respaldo a la innovación tecnológica.

## 1.2. Naturaleza

- **Fases de implementación:** ChaseMyCash recolecta, guarda, procesa y utiliza información personal desde la recopilación inicial de datos de los usuarios hasta su almacenamiento y análisis subsiguientes para proporcionar servicios financieros personalizados.
- **Flujo de información personal:** La información personal circula a través de diversas tecnologías, desde el frontend hasta el backend, atravesando diferentes aplicaciones y servicios consumidos como parte del servicio.
- **Operaciones de tratamiento:** Se llevan a cabo tanto operaciones de manejo manuales como automatizadas, como el registro de usuarios, la gestión de permisos, la recolección de datos de transacciones, el análisis de datos para ofrecer servicios personalizados, entre otros.
- **Activos/Elementos donde se implementa:** La gestión de datos se ejecuta en distintos componentes y activos, como servidores en la nube de AWS, aplicaciones y servicios externos como Zoho CRM, Pumble, MailChimp y Trello.
- **Roles con acceso a los datos:** Los roles que acceden a los datos principalmente incluyen empleados de ChaseMyCash, como administradores y gestores, además de los propios usuarios de la aplicación.
- **Características tecnológicas relevantes:** La tecnología empleada por ChaseMyCash abarca servicios en la nube de AWS, Docker, NodeJS, Python, Vue.js, HTML, CSS, JavaScript, jQuery, y bibliotecas como BootstrapVue y AWS-SDK.
- **Participación de terceros:** Esto puede involucrar almacenamiento de datos en S3 o procesamiento de pagos a través de proveedores externos.

## 1.3 Ámbito/Alcance

- **Extensión en el volumen de información:** La gestión de datos comprende datos personales de los usuarios inscritos en la plataforma, como sus nombres, apellidos, direcciones de correo electrónico, contraseñas encriptadas, detalles financieros y registros de transacciones. Este conjunto de datos se extiende a lo largo de los 20.000 clientes distribuidos globalmente, lo que representa una considerable cantidad de información.
- **Extensión en el número de personas afectadas:** Tal como se mencionó previamente, la cantidad de 20.000 clientes representa un grupo considerable, si bien es posible que en un futuro cercano esta cifra experimente un aumento significativo.
- **Extensión en la diversidad y clasificación de los datos:** La gestión implica la manipulación de información personal que abarca aspectos como nombres, apellidos, direcciones de correo electrónico, contraseñas encriptadas, así como datos financieros que incluyen números de tarjetas de crédito y registros de transacciones
- **Extensión en el alcance geográfico:** Aunque ChaseMyCash tiene su enfoque principal en Europa y aloja sus servidores en la región de Frankfurt, Alemania, su plataforma está abierta para ser utilizada por usuarios de cualquier parte del mundo.
- **Extensión en la duración del procesamiento:** La manipulación de los datos de los usuarios se realiza durante el período en el que estos continúen utilizando la aplicación.
- **Extensión en la duración de retención:** ChaseMyCash conserva de manera indefinida los datos almacenados en su sistema, sin implementar una política de eliminación.
- **Frecuencia de recolección:** La recolección de datos varía según las transacciones y operaciones financieras efectuadas por los usuarios.
- **Granularidad:** Los datos manejados por ChaseMyCash tienen una alta granularidad, ya que incluyen información financiera y personal detallada de los usuarios.

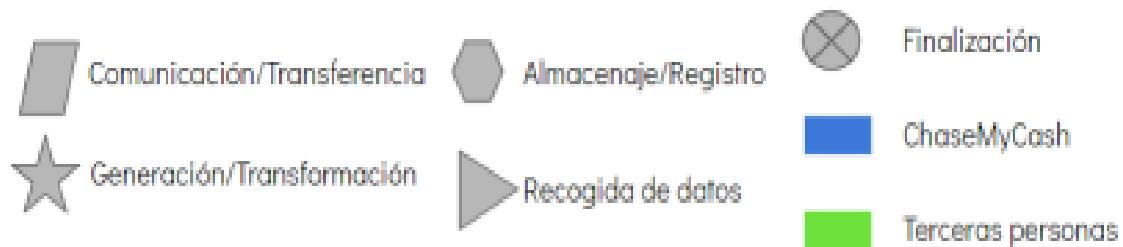
## 1.4 Contexto

- **Mercado o sector en el que opera:** ChaseMyCash se encuentra en el cruce entre los sectores financiero y tecnológico, ofreciendo soluciones innovadoras para la gestión financiera de pequeñas y medianas empresas.
- **Entorno social en el que se despliega:** Su contexto social es una sociedad cada vez más digitalizada, orientada hacia la eficiencia y la automatización en los procesos empresariales.
- **Marco normativo:** La empresa está sujeta a cumplir con regulaciones y normativas sobre tratamiento de datos personales, protección de la privacidad y seguridad de la información en el sector financiero y tecnológico.
- **Interacción con otros sistemas internos:** ChaseMyCash puede interactuar con sistemas y aplicaciones internas de la empresa, como los sistemas contables o de facturación.
- **Cesiones de datos necesarias:** En ciertas ocasiones, se requiere ceder datos a terceros, como instituciones financieras para la gestión de pagos.
- **Transferencias internacionales implicadas:** Al desplegar su producto en la región "Europe (Frankfurt) - eu-central-1" de Amazon, ChaseMyCash puede involucrar transferencias internacionales de datos.
- **Efectos secundarios en la sociedad:** La aplicación de ChaseMyCash puede generar un impacto positivo en la economía y la eficiencia empresarial, aunque también puede tener efectos secundarios como la automatización de procesos, lo que podría resultar en la pérdida de empleos.

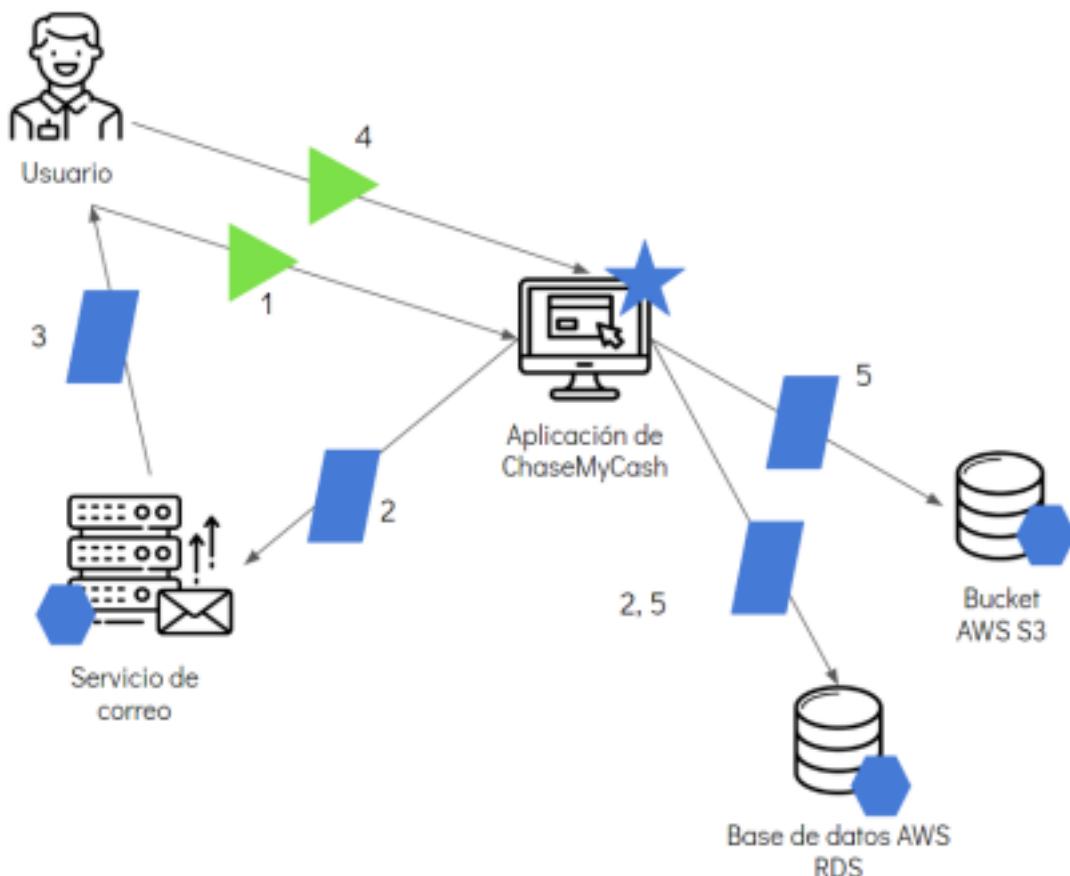
## 2. Flujos de datos

La compañía ChaseMyCash proporciona a sus usuarios un servicio para administrar sus finanzas personales, lo que les permite supervisar sus gastos, analizar su situación financiera y tomar decisiones informadas para mejorar su bienestar financiero. Para asegurar el funcionamiento adecuado del servicio, se requieren datos personales (como correo electrónico, nombre, facturas, cuentas bancarias, etc.). Además, con la licencia "Large", se contempla la posibilidad de utilizar datos biométricos al permitir el uso del doble factor de autenticación.

A continuación, se presentan dos escenarios de uso en los que se manipulan datos personales.

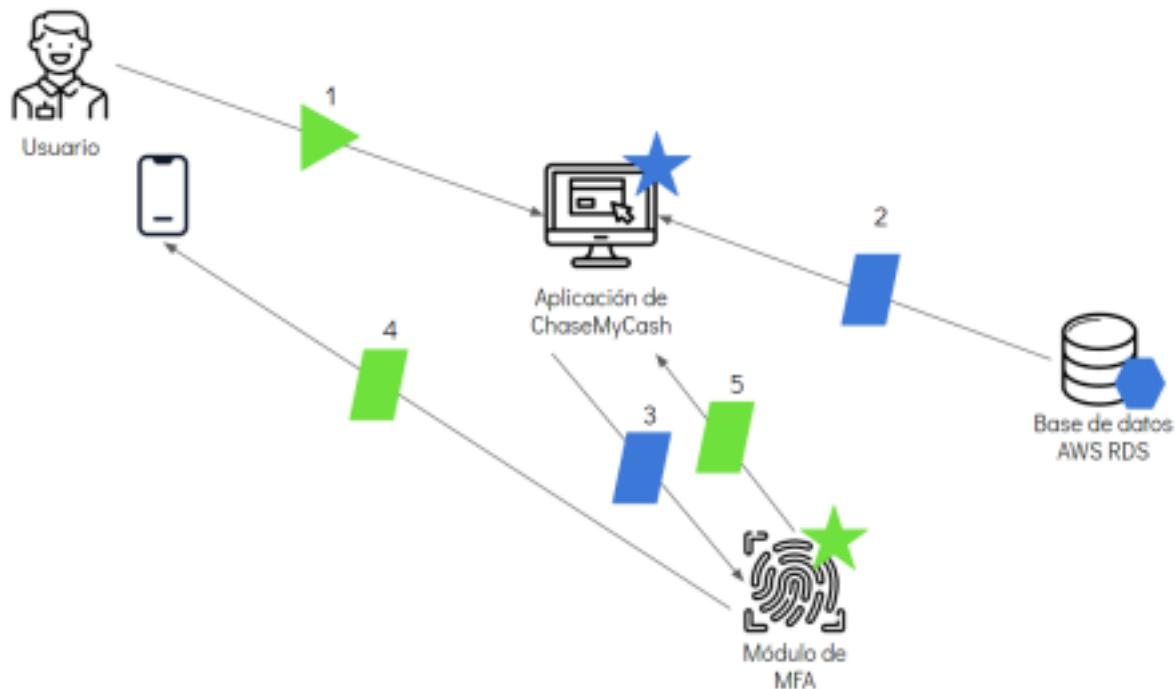


## Registro de usuario



1. Un usuario interesado en los servicios de ChaseMyCash accede a la aplicación web, elige la licencia deseada, selecciona las opciones de pago y proporciona una dirección de correo válido
2. La aplicación genera automáticamente una contraseña temporal y la guarda en la base de datos.
3. Utiliza el servicio de correo AWS SES para enviar al usuario la contraseña temporal para su primer acceso.
4. Se solicita al usuario que ingrese detalles sobre su situación personal (estado civil, número de personas a su cargo, tipo de vivienda), situación laboral (tipo de contrato, antigüedad en el empleo) y situación financiera (bancos con los que opera, productos financieros contratados). Además, se le requiere cargar un archivo XLS o CSV con los movimientos bancarios de sus cuentas de los últimos seis meses como mínimo, para contar con un historial detallado.
5. Después de utilizar la clave provisional por primera vez, se le pide al usuario que genere una nueva contraseña, la cual será almacenada en la base de datos junto con la información proporcionada sobre su situación personal, laboral y financiera

## Acceso al servicio haciendo uso del doble factor de autenticación



1. El usuario transmite sus credenciales de inicio de sesión a la plataforma de ChaseMyCash y solicita acceso.
2. La plataforma extrae de la base de datos RDS la información requerida para el inicio de sesión.
3. La plataforma se comunica con el módulo de autenticación de doble factor, enviándole los datos necesarios para el inicio de sesión.
4. El módulo de doble factor solicita al usuario el segundo factor de autenticación.
5. El módulo de autenticación devuelve a la plataforma los resultados de las comparaciones. Según el resultado:
  - Si es afirmativo, la plataforma permite al usuario acceder.
  - Si es negativo, la plataforma deniega el acceso.

Clasificación de los agentes que participan en los flujos de datos anteriores:

RECOGIDA DE DATOS	GENERACIÓN/ TRANSFORMACIÓN	ALMACENAMIENTO DE DATOS
 Usuario	 Aplicación de ChaseMyCash	 Base de datos AWS RDS
	 Módulo de doble factor de autenticación	 Bucket AWS S3
		 Servicio de correo

### 3. Análisis de riesgos que afectan a la privacidad

En esta sección, se realizará un análisis exhaustivo de los posibles riesgos que podrían afectar a la privacidad, siguiendo las directrices de la Agencia Española de Protección de Datos. Este análisis es esencial para asegurar que se están implementando las medidas adecuadas para proteger la privacidad de las personas y prevenir cualquier brecha de datos personales. Para cada riesgo identificado, se establecerá un nivel de impacto y probabilidad, lo que permitirá evaluar la gravedad del riesgo de manera más precisa. Utilizaremos la matriz de "Probabilidad x Impacto" proporcionada por la AEPD para llevar a cabo esta evaluación. La combinación de los niveles de impacto y probabilidad nos ayudará a determinar el nivel de riesgo cualitativo asociado con cada peligro.

Probabilidad	Muy alta	Medio	Alto	Muy alto	Muy alto
	Alta	Bajo	Alto	Muy alto	Muy alto
	Baja	Bajo	Medio	Alto	Muy alto
	Improbable	Bajo	Bajo	Medio	Muy alto
		Muy limitado	Limitado	Significativo	Muy significativo
Impacto					

Tabla 14 Matriz Probabilidad x Impacto para determinar el nivel de riesgo

Es fundamental destacar que la clasificación de los niveles de riesgo seguirá el orden de bajo, medio, alto y muy alto. Esto facilitará la identificación y priorización de los riesgos más críticos para asegurar que se implementen las medidas de mitigación necesarias y se prevenga cualquier daño a la privacidad de las personas afectadas. En síntesis, este proceso permitirá tomar decisiones más fundamentadas y adoptar las medidas adecuadas para salvaguardar la privacidad de los individuos.

### 3.1 RIESGO DE TRATAMIENTO EXCESIVO

<b>El volumen de datos tratados es muy elevado</b>	<b>Muy Alto</b>
<b>La duración del tratamiento es elevada</b>	
P.ej. y sin ser exhaustivos: • La permanencia del tratamiento es elevada • Otros	<b>Medio</b>

Para evaluar este riesgo, primero consideraremos la probabilidad de que ocurra. Dado que ChaseMyCash mantiene los datos almacenados de forma permanente sin una política de eliminación, lo cual aumenta la posibilidad de filtraciones de datos sensibles, clasificaremos la probabilidad como **alta**.

Luego, evaluaremos el impacto potencial de este riesgo. Dado que la falta de eliminación frecuente de datos puede provocar filtraciones masivas de información sensible, el impacto sería **significativo** en términos de daño a la privacidad de los clientes y la reputación de la empresa.

Por lo tanto, este riesgo se clasifica como de alta probabilidad y alto impacto, lo que lo sitúa en la categoría de riesgo alto. Es esencial que ChaseMyCash establezca políticas de retención de datos adecuadas para mitigar este riesgo y garantizar la protección de la privacidad de los clientes.

### 3.2 RIESGO DISCRIMINACION POR LA SITUACIÓN ECONÓMICA

Situación económica P.ej. sin ser exhaustivos: <ul style="list-style-type: none"><li>• Renta personal</li><li>• Ingresos mensuales</li><li>• Patrimonio (bienes muebles/inmuebles)</li><li>• Situación laboral</li><li>• Otros</li></ul>	Medio
Estado financiero P.ej. sin ser exhaustivos: <ul style="list-style-type: none"><li>• Solvencia financiera</li><li>• Capacidad de endeudamiento</li><li>• Nivel de deuda (Préstamos personales, hipotecas)</li><li>• Listas de solvencia</li><li>• Impagos</li><li>• Activos (fondos de inversión, rendimientos generados, acciones, cuentas a cobrar, rentas percibidas, etc.)</li><li>• Pasivos (gastos en alimentación, vivienda, educación, salud, impuestos, pagos de créditos, tarjetas de crédito o gastos personales, etc.; o deudas u obligaciones</li><li>• Otros</li></ul>	Medio

En este escenario planteado, existe un riesgo potencial significativo para los clientes que utilizan los servicios de ChaseMyCash. Una filtración de datos financieros personales podría ser aprovechada de manera malintencionada para perjudicar a los afectados. Una de las posibles consecuencias sería la discriminación financiera en el futuro, ya que las empresas podrían tomar decisiones de préstamo o financiamiento basadas en la solvencia financiera de los solicitantes.

Si los datos financieros de una persona se ven comprometidos debido a la filtración, podría enfrentar la negación de ciertos beneficios o oportunidades económicas. Mientras tanto, otras personas que no han sido afectadas por esta brecha de seguridad podrían tener más éxito en sus solicitudes de préstamos o financiamiento.

Para evaluar la gravedad de este riesgo, debemos considerar tanto la probabilidad de que ocurra como el impacto que tendría si sucediera. Dado que ChaseMyCash maneja datos financieros personales de sus clientes, la probabilidad de una filtración de datos es **muy alta**. Además, el impacto potencial sería **significativo**, ya que los datos financieros personales son altamente confidenciales y su exposición podría tener consecuencias graves para la vida económica del individuo afectado.

### 3.3 RIESGO DE FALTA DE TRANSPARENCIA Y ACCESO A LOS DATOS

<p>Decidir sobre el control del interesado de sus datos personales</p> <ul style="list-style-type: none"><li>• Derecho de acceso.</li><li>• Derecho de rectificación</li><li>• Derecho de oposición</li><li>• Derecho de supresión</li><li>• Derecho de limitación del tratamiento</li><li>• Derecho de no ser sometido a decisiones automatizadas sin intervención humana.</li><li>• Derecho a la portabilidad</li><li>• Otros</li></ul>	Alto
---	------

El riesgo que se analizará implica la posibilidad de que se deniegue el derecho al control de los datos personales del cliente en términos de acceso, rectificación, oposición o supresión. Es crucial que la empresa garantice que los usuarios tengan acceso a sus datos personales y a información clara y transparente sobre su tratamiento. Además, los usuarios deben poder ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición) en relación con sus datos personales. La falta de garantía de estos derechos podría resultar en sanciones y daños a la reputación de la empresa.

La probabilidad de que se deniegue este derecho se considera **alta**, dado que puede ocurrir debido a errores humanos o técnicos, o incluso de forma intencional, especialmente considerando el aparente compromiso limitado de ChaseMyCash con la protección de la privacidad de sus usuarios. Además, el manejo de una gran cantidad de datos personales por parte de ChaseMyCash aumenta la probabilidad de errores o infracciones en la protección de datos.

En cuanto al impacto, se considera **muy significativo**, ya que los datos personales son información sumamente sensible y valiosa para los usuarios. Su mal uso o acceso no autorizado puede tener consecuencias graves para la privacidad y seguridad de los individuos afectados. Además, la denegación de los derechos ARCO puede socavar la confianza y la imagen de la empresa, lo que podría resultar en la pérdida de clientes y en sanciones económicas.

### 3.4 USO DE TERCEROS PROVEEDORES

Internet de las cosas (IoT)	Muy Alto
Uso innovador o nuevas soluciones organizativas	Alto
Uso innovador de tecnologías consolidadas P.ej. y sin ser exhaustivos: <ul style="list-style-type: none"><li>• Tecnologías en las que no se ha evaluado el impacto en la privacidad</li><li>• Tecnologías utilizadas a una nueva escala</li><li>• Otros</li></ul>	Alto
Tecnologías combinadas con otras	Medio

El riesgo que se analizará implica el uso de servicios de terceros proveedores, como el almacenamiento de datos en S3 o el procesamiento de pagos, asegurando que estos proveedores cumplan con las normativas y regulaciones en cuanto al tratamiento de datos personales. Si estos proveedores sufren una violación de datos, ChaseMyCash podría ser responsable de la fuga de información personal de sus clientes. Además, ChaseMyCash utiliza varios otros servicios externos como Zoho CRM, Pumble, MailChimp y Trello, los cuales pueden acceder a los datos personales de los usuarios y comprometer la privacidad de los clientes si no se manejan adecuadamente.

Para evaluar este riesgo, primero determinaremos la probabilidad, que estableceremos como **muy alta** debido a la cantidad de servicios de terceros contratados por la empresa. Cuantos más servicios externos se utilicen, mayor es la probabilidad de que se produzca una fuga de datos.

Por otro lado, después de definir la probabilidad de riesgo, evaluaremos el impacto, que según la línea de probabilidad de riesgo, lo estableceremos como **limitado**. Esto se debe a que estos proveedores suelen emplear métodos de seguridad robustos que ayudan a mitigar intrusiones y evitar fugas de información.

### 3.5 TRANSFERENCIAS INTERNACIONALES DE DATOS

<p>La actividad de tratamiento tiene un gran alcance geográfico P.ej. y sin ser exhaustivos:</p> <ul style="list-style-type: none"><li>• Nivel regional, nacional o supranacional</li><li>• Otros</li></ul>	<p>Medio</p>
---	--------------

El riesgo que implica que ChaseMyCash opere principalmente en Europa, aunque tenga clientes en todo el mundo, se analizará considerando la probabilidad y el impacto.

La probabilidad de este riesgo se establece como **alta**, ya que al desplegar su producto en Europa, puede implicar transferencias internacionales de datos que deben cumplir ciertos requisitos y condiciones establecidos por la legislación aplicable en materia de protección de datos. La transferencia de datos personales a países fuera de la UE sólo puede llevarse a cabo si se cumplen estas condiciones, como el consentimiento explícito de los titulares de los datos y la existencia de garantías adecuadas para proteger la privacidad y seguridad de los datos transferidos.

El impacto de no cumplir con estas condiciones podría ser significativo para ChaseMyCash. Podría vulnerar los derechos de las personas en países concretos y enfrentarse a posibles sanciones y multas por parte de las autoridades de protección de datos. Además, esto podría dañar la reputación y confianza de los clientes en la empresa.

Dada la **alta** probabilidad y el impacto **significativo**, es crucial que ChaseMyCash cumpla con las regulaciones de protección de datos al operar en Europa y al manejar transferencias internacionales de datos para evitar consecuencias adversas para la empresa y sus clientes.

## 4. Mapa de riesgos

PROBABILIDAD	MUY ALTA				
	ALTA				
	BAJA	TRATAMIENTO EXCESIVO  TRANSFERENCIAS INTERNACIONALES DE DATOS	DISCRIMINACIÓN POR SITUACIÓN ECONÓMICA  USO DE TERCEROS PROVEEDORES		
	IMPROBABLE		FALTA DE TRANSPARENCIA Y ACCESO A DATOS		
		MUY LIMITADO	LIMITADO	SIGNIFICATIVO	MUY SIGNIFICATIVO
IMPACTO					

Es evidente que la protección de la privacidad de los datos de los clientes de ChaseMyCash es una preocupación importante, dada la serie de riesgos identificados.

La falta de transparencia y acceso a los datos personales de los clientes podría resultar en sanciones y daños a la reputación de la empresa. Además, el riesgo de filtración de datos y discriminación por situación económica podría tener graves repercusiones para los clientes.

El uso de terceros proveedores también presenta riesgos significativos, ya que podría poner en peligro la privacidad de los clientes de ChaseMyCash si estos proveedores no cumplen con las normativas y regulaciones adecuadas sobre el tratamiento de datos personales.

Finalmente, el riesgo de transferencias internacionales de datos plantea desafíos adicionales, ya que podría vulnerar los derechos de las personas y exponer a la empresa a posibles sanciones y multas.

En resumen, la falta de compromiso por parte de ChaseMyCash en la aplicación de políticas y medidas

de protección de datos adecuadas es preocupante y podría resultar en la exposición de información sensible y valiosa de los clientes. Es fundamental que la empresa tome medidas inmediatas para abordar estos riesgos y garantizar la privacidad y seguridad de los datos de sus clientes.