POLÍTICA DE SEGURIDAD

Referencia del Documento | PL05_PP_V7

ÍNDICE

1. Referencias	Reglamento General de Protección de Datos 2016/679, de 27 de abril de 2016 Decreto-Ley Nº 242/2012, de 7 de noviembre Ley Nº 25/2008, de 5 de junio
2. Documentos Asociados	PL02 - Política de Continuidad de Operaciones PC03 - Proceso de Continuidad de Operaciones PL03 - Política de Gestión de Riesgos de BC y FT PR02 - Procedimiento de Operación Sospechosa o Inusual
3. Lista de Distribución	Todo el personal de PayPay
4. Historial del Documento	2018-06-05|Versión 1 2018-08-16|Versión 2 2018-10-09|Versión 3 2018-10-25|Versión 4 2018-10-31|Versión 5 2019-01-02|Versión 6 2020-06-04|Versión 7
5. Clasificación del Documento	D | Público

6. Registro de la revisión

Nº de la Versión	Elaborado	Aprobado	Motivo
	04-06-2020	**04-06-2020**	
7	***Compliance***	**Gerencia**	Inclusión de información relacionada con la Política de Seguridad de la Información
	Inês Sousa	Tolentino Pereira	

7. Objetivo y Alcance

El objetivo de esta política es definir procedimientos para evitar el uso de PayPay con fines de blanqueo de capitales (BC) y/o financiación al terrorismo (FT), según las características del cliente, así como evitar el posible uso ilícito de datos sensibles y personales. Asimismo, esta política representa el compromiso asumido por PayPay, como institución intermediaria de pagos, con el RGPD vigente.

8. Aplicabilidad

PayPayUE – Instituição de Pagamento, Unipessoal, Lda es una empresa intermediaria de pagos que proporciona a sus clientes, mediante un portal en línea, www.paypay.pt, referencias de pago.

Actualmente dispone de cuatro métodos de pago, a saber: Multibanco (ATM), Multibanco Real Time, Tarjeta de Crédito/Débito Visa/MasterCard y MB WAY.

Paypay solo proporciona este servicio a empresas con NIF portugués y que se encuentren domiciliadas en Portugal.

9. Compromiso con la Seguridad de la Información

- Confidencialidad

Garantizar de que la información de los clientes, cuya custodia es confiada a la plataforma electrónica de PayPay, sea accedida únicamente a quienes estén formalmente autorizados para tal fin.

- Integridad

Garantizar la protección de la exactitud de la información recibida, procesada, almacenada y transmitida bajo responsabilidad de PayPay en su plataforma.

- Disponibilidad

Garantizar que la información manejada sea accesible, cuando sea necesario, para realizar una actividad de tipo comercial, dentro de los niveles de servicio definidos formalmente y respetando el compromiso de confidencialidad e integridad.

- Privacidad de los Datos

Garantizar la privacidad y la confianza de sus titulares y socios, promoviendo una protección total sobre la privacidad y seguridad de los datos personales.

- No Repudio

Garantizar que el autor no niegue haber creado y firmado un documento.

- Autenticidad

Garantizar la validez de la transmisión, del mensaje y de su remitente. La finalidad es que el destinatario pueda probar el origen y la autoría de un documento determinado.

10. Implementación de la Política de Seguridad de la Información

El Coordinador de Sistemas de Gestión es responsable por la definición e implementación de la Política de Seguridad de la Información, Estándares, Procedimientos y Directrices.

Todo el personal es responsable del cumplimiento de las reglas establecidas, así como de comunicar al Coordinador de Sistemas de Gestión cualquier acontecimiento o incidente de Seguridad de la Información que pueda afectar el normal funcionamiento de PayPay.

10.1. Perfiles y Responsabilidades

Los siguientes perfiles del personal están dirigidos a tales fines:

Alta Dirección / Liderazgo – Responsable de coordinar la estrategia de ACIN y coordinar a los responsables de cada departamento del Grupo. El cargo de Alto Directivo es ejercido por el administrador José Luís de Sousa.
Es responsable de la delegación de actividades, la adquisición de cualquier equipo y servicio y de la autorización de nuevas infraestructuras de información.

Coordinador de Sistemas de Gestión – Responsable de garantizar que los procesos, políticas y controles necesario en el ámbito de SGQ, SGSI y SGS sean establecidos, implementados y cumplidos.
Informa al Liderazgo sobre el estado de funcionamiento y las necesidades de mejora de los sistemas de gestión.
Promueve la divulgación y sensibilización de los sistemas de gestión a nivel de todas las unidades de la empresa.

Auditor Interno – Responsable de participar en la realización de Auditorías en los Sistemas de Gestión y en los Procesos, con miras a verificar y evaluar su eficacia y conformidad.
Elabora el plan de Auditoría Interna, el informe de la Auditoria, y presenta sugerencias de mejora.

Coordinador de Proyectos – Responsable de coordinar todos los proyectos de desarrollo de software, y del nombramiento y coordinación del Equipo de Desarrollo.
Igualmente, es responsable del análisis de riesgo y viabilidad de los proyectos, del seguimiento de los procesos de análisis de los requisitos y del modelado de soluciones, del análisis y validación de toda la documentación de modelado/arquitectura creada.

Programadores / Analistas – Responsables de participar en todas las fases del proceso de desarrollo y mantenimiento de software, incluyendo el análisis de los requisitos, el modelado y la arquitectura de la solución, la implementación de la solución, la realización de pruebas y la validación de los requisitos, la creación de manuales y documentación de respaldo y la capacitación de los usuarios, cuando corresponda.

Software Beta Tester – Responsable de realizar pruebas y de probar y validar los requisitos.

Analista de Calidad del Servicio – Responsable de llevar a cabo pruebas y de la validación de los requisitos establecidos, de la creación y revisión del contenido presentado y la realización de auditorías internas a la Oficina de Coordinación del Proyecto en lo que se refiere a las buenas prácticas de desarrollo seguro.

Administrador de Seguridad – Responsable, en términos generales, de implementar las políticas y prácticas de seguridad.

Administrador de Sistemas – Autorizado a instalar, configurar y mantener los sistemas.

Operador de Sistemas - Responsable del funcionamiento diario del sistema desde el punto de vista de la aplicación. Responsable de operar diariamente los servidores que soportan el sistema de la aplicación.

Auditor de Sistemas – Autorizado para monitorear los archivos de actividad del sistema y el registro de eventos para auditoría.

Técnicos de Apoyo – Prestan asistencia y seguimiento técnico a la plataforma.
Los Técnicos de Apoyo tienen como responsabilidad cumplir los procesos y políticas en el marco de los Sistemas de Gestión.

Técnico de Contabilidad – Responsable de la facturación y del control de los documentos contables de ACIN.

Técnico Administrativo – Responsable de la ejecución de varias tareas administrativas, necesarias para el buen funcionamiento de ACIN.

Gestor de Riesgo – Responsable de la identificación, evaluación y tratamiento de riesgos.

Gestor de Capacidad – Responsable de garantizar la disponibilidad permanente de todos los recursos requeridos para mantener la continuidad de operaciones.

Gestor de Incidentes de Seguridad de la Información – Responsable de garantizar un enfoque coherente y efectivo para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de incidentes y debilidades de seguridad.

Gestor de Criptografía - Responsable de desarrollar e implementar la Política sobre el uso de controles criptográficos.

Gestor de Redes y Comunicaciones - Responsable de la gestión y control de redes de comunicaciones para la protección de la información.

Gestor de Sistemas Informáticos - Responsable de la gestión y control de los sistemas informáticos.

Gestor de Proveedores – Responsable de gestionar la relación con los proveedores.
El Gestor de Proveedores es responsable del cumplimiento de los procesos y políticas en el marco del SGSI.

Gestor de Continuidad de Operaciones – Responsable de asegurar el funcionamiento continuo de la organización y la recuperación oportuna de su actividad.

Gestor de Conformidad de las Plataformas de Aplicaciones – Responsable de coordinar todos los proyectos de desarrollo de software.

Gestor de Auditorías – Responsable de participar en la Auditoría de los Sistemas y Procesos de Gestión de Seguridad de la Información, con el fin de verificar y evaluar su efectividad y cumplimiento.

11. Medidas de Seguridad de PayPay

11.1. Identificación de Datos Sensibles de Pago en PayPay

Teniendo en cuenta los métodos de pago de cajero automático (Multibanco), tarjetas de crédito/débito y MBWAY, hemos identificado como datos de pago sensibles los siguientes:

I. IBAN del cliente
II. Número máximo de Referencias Diarias
III. Importe máximo por referencia
IV. Importe máximo diario
V. Precios

11.2. Protección de los Servicios

PAYPAYUE utiliza del protocolo de seguridad 3D Secure. El protocolo 3D Secure fue desarrollado por las principales marcas de Tarjetas de Crédito/Débito y hace posible la autenticación inequívoca de todos los participantes en una transacción de comercio electrónico. Este protocolo es empleado por VISA, bajo el nombre de Verified by Visa, y por Master Card, bajo el nombre de Secure Code. De esta forma, cuando un cliente realiza un pago en el portal www.paypay.pt se activa un proceso de verificación de la validez de la Tarjeta de Crédito/Débito.

Los sistemas de seguridad vinculados al protocolo 3D Secure validan la identidad del cliente e informan al portal www.paypay.pt sobre la legalidad de la tarjeta utilizada para el pago. De esta manera, es posible eliminar el fraude y los costos y pérdidas asociados con estas situaciones. Todo este proceso se realiza de manera automática y absolutamente transparente. La protección proporcionada por este protocolo, es decir, en compras fraudulentas, está totalmente garantizada. PayPay se compromete a responder en un plazo máximo de dos (2) días laborables cualquier solicitud presentada por los usuarios de las tarjetas.

El portal www.paypay.pt utiliza el protocolo criptográfico de seguridad (TSL) para salvaguardar la seguridad y confidencialidad de los datos ingresados por el usuario (Art. 76º). Es completamente seguro ingresar los datos de su Tarjeta de Crédito/Débito en cualquier pago realizado en www.paypay.pt, ya que todos los datos son ingresados en un Servidor Seguro (TSL de 256 bits) que encripta/codifica (es decir, transforma en un código) todos los datos confidenciales relativos a su Tarjeta de Crédito/Débito.

PayPayUE – Instituição de Pagamento, Unipessoal, Lda. garantiza que no alquila o vender los datos de sus clientes a terceros (Art. 32º), por lo que todas las informaciones son confidenciales y utilizadas únicamente por PayPayUE – Instituição de Pagamento, Unipessoal, Lda. para el procesamiento de los pagos y el envío eventual de comunicaciones que refuerce y personalice la oferta cultural o de productos.

Diariamente, PayPay promueve la mejora continua de las políticas y de los procedimientos internos con miras a la prevención del blanqueo de capitales y de financiación del terrorismo. Este tipo de actividades se materializa en el cumplimiento de las leyes y reglamentos aplicables, por el respeto a los principios éticos y por la adopción de las buenas prácticas internacionalmente adoptadas, según lo estipulado en la Ley Nº 25/2008, del 5 junio.

El personal de la empresa está obligado al estricto cumplimento de todos los deberes consagrados en el ordenamiento jurídico en vigor, particularmente con los deberes de análisis y de comunicación de todas las operaciones que puedan presentar riesgo de BC y/o FT, siendo la capacitación unos de los aspectos fundamentales de todo el sistema de prevención.

Para la verificación y confirmación de la viabilidad y veracidad de los datos suministrados, antes de activar las cuentas de los clientes, se solicita el envío de copia del documento de identidad del cliente individual y de la empresa a la cual pertenece, de conformidad con las directrices del Banco de Portugal (entidad supervisora de las actividades de las instituciones financieras, según el Decreto Ley 242/2012).

11.3. Garantía de Pagos Seguros

Siempre que se desee cambiar, añadir o eliminar un IBAN para recibir fondos, deberá hacerlo el representante legal de la entidad definido en PayPay.

De esta manera, únicamente los clientes pueden solicitar el cambio del IBAN, excluyendo la posibilidad de que un empleado de PayPay altere la cuenta por error o incluso intencionalmente, reduciendo la posibilidad de fraude.

La solicitud se realiza directamente en www.paypay.com, después de la autenticación del cliente. Cuando se produzca una solicitud de modificación o adición de un nuevo IBAN, se envía una alerta por correo electrónico al *Compliance*. El documento de respaldo de IBAN debe ser enviado por el representante legal de la empresa que realizó esta solicitud en la plataforma, para garantizar que:

- Efectivamente el representante legal solicitó la modificación del IBAN;
- Que el IBAN registrado pertenezca a la entidad.

Después de confirmación por escrito, el *Compliance* aprueba el IBAN, adjuntando el documento acreditativo en la ficha del cliente en la plataforma.

Debido al procedimiento implementado por PayPay, el cliente solo puede solicitar el cambio, pero no puede, de ninguna forma, modificar efectivamente el IBAN directamente en la plataforma, ya que esto requiere, obligatoriamente, la validación de PayPay.

11.4. Control de Clientes de Alto Riesgo

Cuando PayPay recibe del Banco de Portugal información relativa a un cliente considerado de alto riesgo, PayPay registra esa información en la plataforma, de modo que, si un cliente incluido en esta lista se registra, la plataforma emite una alerta en el formulario de aprobación del cliente y bloquea la aprobación de este cliente.

En el caso de que se trate de un cliente ya registrado que utiliza PayPay, al ingresar los datos como Cliente de alto riesgo, la plataforma emite una alerta al *Compliance*, para que este pueda informar al cliente y desactivar los accesos a PayPay.

11.5. Monitoreo y Medición de Operaciones

El monitoreo y la medición de las operaciones de control de PayPay se llevan a cabo utilizando los siguientes indicadores:

I. Importe mensual recibido superior al promedio mensual del cliente;
II. Importe mensual recibido inferior al promedio mensual del cliente;
III. Cobros por referencia;
IV. Número de cobros por mes.

11.5.1. Emisión de Notificaciones

La plataforma envía alertas al *Compliance*, por correo electrónico y al TOC, en su ausencia, siempre que haya sospecha de operaciones relacionadas con BC/FT, previamente definidos en la plataforma, a saber:

V. Aumento de más del 40% de los importes recibidos, en un mes determinado;
VI. Importe recibido inferior al 40 % del promedio mensual;
VII. Transacciones ocasionales por un importe igual o superior a 3.000,00€;
VIII. Recepción de 300 o más pagos mensuales en una entidad, salvo excepciones establecidas en el perfil del cliente.

Siempre que se detecte alguno de los indicadores mencionados anteriormente, el *Compliance* de PayPay deberá comunicar esa información a la entidad supervisora de las Instituciones de Pago.

12. Gestión del Riesgo

Con el fin de garantizar la disponibilidad y el cumplimiento del sistema de control interno, PAYPAY se compromete a identificar, analizar, calificar y abordar el riesgo derivado de diversas fuentes de amenazas a sus compromisos.

La Política de Gestión de Riesgos de BC/FT establece la metodología adoptada para tratar los riesgos identificados, en base a las mejores prácticas definidas por los estándares internacionales de referencia, constituyendo, de esta forma, una herramienta de gestión de la empresa.

12.1. Identificación de los Principales Riesgos

Teniendo en cuenta que es una plataforma totalmente web, alojada y desarrollada utilizando *Cloud Computing* como paradigma de funcionamiento, se ha identificado un conjunto de escenarios genéricos que pueden tener un impacto en la actividad de PAYPAYUE, a saber:

- Falla en los Sistemas de Información;
- Ausentismo Laboral;
- Falla en la Seguridad de la Información y/o Actos Maliciosos;

- Falla en los Proveedores de la cadena de valor;
- Falla o indisponibilidad de la estructura física / Desastres Naturales (incendios, anomalías meteorológicas);

Ante alguno de estos incidentes, el primer objetivo siempre será salvaguardar la integridad física de los empleados de PAYPAYUE y restaurar rápidamente los servicios a su funcionamiento normal.

12.2. Análisis del Impacto en las Operaciones

Tras la ocurrencia de un incidente, será necesario evaluar los daños producidos por la situación anómala. A tal fin, se abordará lo siguiente:

- Causa de la situación anómala;
- Área de PayPay afectada;
- Estado de la infraestructura física (estado de los sistemas de suministro eléctrico);
- Condiciones de funcionamiento de la infraestructura tecnológica de PayPay (equipos de Tecnología de la Información -TI- y de comunicaciones);
- Potencial del incidente para causar pérdidas o daños adicionales;
- Tiempo estimado para recuperar las condiciones normales de funcionamiento.

Las situaciones no mencionadas carecen de un análisis del *Compliance*.

Los resultados de la evaluación de daños y su impacto en la organización deberán compararse con los criterios de activación del Plan de Continuidad de Servicios, los cuales son:

Tipología	Descripción del criterio
Edificio	Falta de acceso físico al edificio o de evacuación del edificio
	El edificio sede de PayPay no garantiza la seguridad necesaria para su habitabilidad
Legal	Investigación reglamentaria formal o indagación.
	Cualquier incidente que pueda afectar nuestra capacidad de cumplir con las obligaciones legales o reglamentarias y/o que pueda afectar nuestra licencia como operador.
Pérdida/Violación de Datos	Cualquier incidente que ponga en riesgo la marca o reputación de la organización como resultado de una pérdida grave de datos y/o acceso no autorizado a nuestras redes o sistemas.
Nivel de indisponibilidad del servicio	Cuando la extensión de los daños sufridos por la infraestructura tecnológica de PayPay causa una interrupción en la operación de los equipos de TI o de comunicaciones que soportan los servicios más críticos, previéndose que esa interrupción exceda el tiempo máximo permitido para su reparación.

12.3. Evaluación de Impacto

Los riesgos que pueden derivarse de las eventuales fallas poseen, en general, bajas probabilidades de ocurrencia, pero los impactos negativos que puedan derivarse de ellas pueden poner en peligro, total o parcialmente, el funcionamiento de la empresa durante un largo período, si no se implementan medidas preventivas.

Todos los riesgos y amenazas tienen diferentes recursos relacionados, lo que promueve una evaluación diferenciada según su determinado nivel riesgo. La siguiente tabla presenta el promedio de los valores de cada riesgo, tomados de la Matriz de Análisis de Riesgo (DS07)

Proceso de Evaluación de Riesgos				
Identificación de los Riesgos	**Análisis de Riesgos**			**Tiempos de Respuesta**
	Probabilidad	**Consecuencia**	**Nivel de Riesgo**	
Falla en los Sistemas de Información	C	3	III	R.T.O. < 4h
Ausentismo Laboral	C	1	V	R.T.O. < 4h
Falla en la Seguridad de la Información y/o Actos Maliciosos	B	3	III	R.P.O. < 24h R.T.O. < 4h
Falla en los Proveedores de la cadena de valor	B	3	III	R.T.O. < 4h
Falla o indisponibilidad de la estructura física	B	2	III	R.P.O. < 24h R.T.O. < 4h M.A.O. < 48h
Desastres Naturales (incendios, anomalías meteorológicas)	B	4	II	R.T.O. < 4h

Nivel de Riesgo

Nivel	Prioridad	Acciones de Mitigación
I (Muy Alto)	1 (máxima)	Es obligatorio que el riesgo ya se haya tratado o que se esté ejecutando al menos una MTR.
II (Alto)	2	Es obligatorio que se planifique la ejecución de al menos una MTR antes de la revisión del sistema por parte de la gerencia.
III (Medio)	3	La responsabilidad del monitoreo sistemático se atribuirá al encargado del riesgo, y el *Compliance* será notificado inmediatamente de todas las situaciones que puedan elevar el nivel de riesgo.
IV (Bajo)	4	El *Compliance* enviará una comunicación a los encargados del riesgo, sobre su existencia y sobre la necesidad de supervisarlo en intervalos regulares.
V (Muy Bajo)	5 (mínima)	El *Compliance* enviará una comunicación a los encargados del riesgo sobre la necesidad de revisar su estado al menos una vez al año.

12.4. Plan de Mitigación de los Principales Riesgos

a) **Falla en los Sistemas de Información –** En casos de indisponibilidad del servicio debido a fallas del centro de datos/infraestructura técnica que respalda el sistema, la empresa garantiza la existencia de redundancia de los elementos críticos de la plataforma, entre ellos, base de datos, fuente de alimentación y comunicaciones; garantiza una copia de seguridad de la base de datos; posee una disponibilidad global de la solución de un 99,8 % y una disponibilidad especifica en horario laborable, de las 09 horas a las 19 horas, de un 99,9 %; garantiza la existencia de un centro alternativo para la recuperación en caso de desastre, con activación, en un plazo de 72 horas; y garantiza el monitoreo y funcionamiento de la solución 24x7x365, con un tiempo de intervención técnica en el local de alojamiento inferior a las 2 horas.

   En caso de falla o indisponibilidad debido a la puesta en operación de nueva versión, se realiza una copia de seguridad completa antes del proceso de actualización. Si se identifica alguna no conformidad, el sistema se reinicia utilizando el script de actualización. Este proceso dura un máximo de 60 minutos.

   PAYPAYUE está alojada en el Centro de Datos de ONI, en Máquinas Virtuales, cuyos sus servidores se encuentran repartidos en tres ubicaciones. En caso de un desastre total del Centro de Datos en el cual se encuentra alojada la aplicación, y la aplicación no estuviera disponible, se realiza una llamada telefónica al servicio de apoyo de ONI. Si después de esa llamada se confirma que hubo un desastre en el Centro de Datos, la gerencia emite una orden para que ONI restaure las copias de seguridad del día anterior para que funcionen en alguno de los otros dos Centros de Datos. Los DNS y las redirecciones también se modifican para que reflejen a la nueva ubicación.

b) **Ausentismo Laboral -** En el caso de un brote de gripe, o similar, que reduzca o amenace con infectar una gran parte de los recursos humanos, se asignará acceso remoto a través de VPN a los empleados y, dado que todos tienen acceso a Internet, podrán conectarse a las oficinas de la empresa y continuar realizando sus funciones. Incluso, podrán asignarse teléfonos VoIP preconfigurados para continuar recibiendo y haciendo llamadas a través de las oficinas de PayPay.

c) **Falla en la Seguridad de la Información y/o Actos Maliciosos** - La empresa garantiza la calidad de la información, evitando el acceso a la información a personas no autorizadas y evitando que los datos sean alterados o eliminados sin permiso, mediante la creación de accesos individuales.

d) **Falla o indisponibilidad de la Estructura Física / Desastres Naturales (incendios, anomalías meteorológicas)** - En caso de fallas en la infraestructura o la ocurrencia de desastres naturales (incendios, terremotos, inundaciones) y la destrucción de las oficinas, la base de operaciones se traslada al domicilio particular de la gerencia de la empresa, localizada en Rua 6 de Maio, Nº 11, Ribeira Brava. Ese domicilio cuenta con Internet y áreas para alojar a los empleados que realizan las tareas más críticas para mantener el funcionamiento de la empresa. Se encuentra a menos de 3 minutos a pie de las instalaciones actuales de ACIN, lo que permite la coordinación de las operaciones de reconstrucción/recuperación de la oficina.

13. Gestión de Incidentes y Gestión de la Continuidad de las Operaciones

Todos los eventos que pongan en peligro los compromisos de seguridad de la información y la actividad de PayPay se tratarán como posibles incidentes y, como tales, se incluirán en el proceso de gestión de incidentes de PayPay.

El diagnóstico respectivo de las causas, consecuencias, medidas de control y mitigación de los riesgos que surjan se tratará de acuerdo con las mejores prácticas, con la activación de procedimientos disciplinarios y acciones legales para aquellos asuntos que se califiquen como dolo o incumplimiento de las responsabilidades asumidas por terceros.

La disponibilidad de la información, sin descuidar la responsabilidad sobre el resto de los compromisos de seguridad de la información, se garantizará mediante la implementación de respuestas a incidentes disruptivos incluidos en el ámbito del Proceso de Continuidad de Operaciones de PAYPAY.

14. Capacitación y Sensibilización

La concientización, capacitación y formación sistemática de los empleados de PAYPAY, en materia de seguridad de la información, blanqueo de dinero y/o financiación del terrorismo es un compromiso firme de la empresa.

15. Divulgación y Publicación

La divulgación de la formalización de las decisiones del Liderazgo de PayPay se garantiza a través de la Política de Comunicación.

La publicación interna de documentos relevantes para el funcionamiento de la seguridad de la información se considera esencial a fin de que los empleados de la empresa se sientan corresponsables y cumplan y apliquen las directrices establecidas en ese sentido.