POLÍTICA DE SEGURANÇA

Referência do Documento | PL05_PP_V7

ÍNDICE

1. Referências 3
2. Documentos Associados 3
3. Lista de Distribuição 3
4. Histórico do Documento 3
5. Classificação do Documento 3
6. Registo da revisão 3
7. Objetivo e Âmbito 4
8. Aplicabilidade 4
9. Compromisso para a Segurança da Informação 4
10. Implementação da Política de Segurança da Informação 5
10.1. Perfis e Responsabilidades 5
11. Medidas de segurança da PayPay 7
10.2. Identificação de Dados Sensíveis de pagamento na PayPay 7
10.3. Proteção dos serviços 7
10.4. Garantia de Pagamentos seguros 8
10.5. Controlo de clientes de elevado risco 8
10.6. Monitorização e medição de operações 9
10.5.1. Emissão de notificações 9
12. Gestão do Risco 9
11.1. Identificação dos principais riscos 9
11.2. Análise do impacto no negócio 10
11.3. Avaliação do Impacto 11
11.4. Plano de mitigação dos principais riscos 12
13. Gestão de Incidentes e Gestão da Continuidade de Negócio 13
14. Formação e sensibilização 13
15. Divulgação e publicação 13

1. Referências	Regulamento Geral de Proteção de Dados 2016/679, de 27/04/2016 Decreto-Lei n.º 242/2012, de 7 de novembro Lei n.º 25/2008, de 5 de junho
2. Documentos Associados	PL02- Política de Continuidade de Negócio PC03 - Processo de Continuidade de Negócio PL03 - Política de Gestão de Risco de BC e FT PR02 - Procedimento de Operação Suspeitas ou invulgares
3. Lista de Distribuição	Todos os colaboradores da PayPay
4. Histórico do Documento	2018-06-05|Versão 1 2018-08-16|Versão 2 2018-10-09|Versão 3 2018-10-25|Versão 4 2018-10-31|Versão 5 2019-01-02|Versão 6 2020-06-04|Versão 7
5. Classificação do Documento	D | Público

6. Registo da revisão

N.º da Versão	**Elaborado**	**Aprovado**	**Motivo**
	04-06-2020	**04-06-2020**	
7	***Compliance***	**Gerência**	Inserção de informação relativa à Política de Segurança da Informação
	Inês Sousa	Tolentino Pereira	

7. Objetivo e Âmbito

O objetivo desta política é definir procedimentos permitam prevenir a utilização da PayPay para fins do branqueamento de capitais (BC) e/ou financiamento do terrorismo (FT), baseando-se nas características do cliente, assim como na eventual utilização ilícita de dados sensíveis e pessoais. Neste sentido, esta política representa também o compromisso assumido pela PayPay, enquanto instituição intermediária de pagamentos, com o RGPD em vigor.

8. Aplicabilidade

A PayPayUE – Instituição de Pagamento, Unipessoal, Lda é uma empresa mediadora de pagamentos que disponibiliza por meio de um portal on-line, www.paypay.pt a geração de referências de pagamento para os seus clientes.
Neste momento tem quatro métodos de pagamento, nomeadamente Multibanco, Multibanco Real Time, Cartão de crédito/débito Visa/Mastercard e MB WAY.
A Paypay apenas disponibiliza este Serviço a empresas com NIF português e que estejam sedeadas em Portugal.

9. Compromisso para a Segurança da Informação

- Confidencialidade

Garantia de que a informação de clientes que é confiada à custódia da plataforma eletrónica da PayPay é acedida apenas a quem está formalmente autorizado para esse efeito.

- Integridade

Garantia de proteção da exatidão da informação recebida, processada, armazenada e transmitida por responsabilidade da PAYPAY na sua plataforma.

- Disponibilidade

Garantia de que a informação tratada está acessível, e quando necessário, para realizar uma atividade de um processo de negócio, dentro dos níveis de serviço definidos formalmente, e respeitando o compromisso de confidencialidade e integridade.

- Privacidade de Dados

Garantia da privacidade e a confiança dos seus titulares e parceiros, promovendo a total proteção sobre a privacidade e segurança dos dados pessoais.

- Não Repúdio

Garantir que o autor não negue ter criado e assinado o documento

- Autenticidade

Garantir que a validade da transmissão, da mensagem e do seu remetente. O objetivo é que o destinatário possa comprovar a origem e autoria de um determinado documento.

10. Implementação da Política de Segurança da Informação

O Coordenador de Sistemas de Gestão é responsável pela definição e implementação da Política de Segurança da Informação, Standards, Procedimentos e *Guidelines*.

Todos os Colaboradores são responsáveis pela observância das regras definidas, bem como por comunicar ao Coordenador de Sistemas de Gestão qualquer evento ou incidente de Segurança da Informação que possa afetar o normal funcionamento da PayPay.

10.1. Perfis e Responsabilidades

Estão afetos a este âmbito os seguintes perfis de colaboradores:

Gestão de Topo / Liderança – Responsável pela coordenação da estratégia da ACIN e coordenação dos responsáveis por cada departamento do grupo. O cargo de Gestor de Topo é assumido pelo administrador Tolentino Pereira.
É responsável pela delegação de atividades, aquisição de qualquer equipamento e serviço e pela autorização de novas infraestruturas de informação.

Coordenador de Sistemas de Gestão – Responsável por garantir que os processos, políticas e controlos necessários no âmbito do SGQ, SGSI e SGS são estabelecidos, implementados e cumpridos.
Reportar à Liderança o estado da performance e necessidades de melhoria dos sistemas de gestão.
Promover a divulgação e sensibilização dos sistemas de gestão ao nível de todas as unidades da empresa.

Auditor Interno – Responsável por participar na realização de Auditorias aos Sistemas de Gestão e aos Processos, a fim de verificar e avaliar a sua eficácia e conformidade.
Realização do plano de Auditoria Interna, do relatório da Auditoria, e apresentação de sugestões de melhoria.

Diretor de Projetos – Responsável por coordenar todos os projetos de desenvolvimento de software, e pela nomeação e coordenação da Equipa de Desenvolvimento.
É também responsável pela análise de risco e viabilidade dos projetos, pelo acompanhamento dos processos de análise de requisitos e modelação da solução, pela análise e validação de toda a documentação de modelação/arquitetura criada.
É responsável pela análise dos pedidos de melhoria/retificação de funcionamento e pela formação de utilizadores, sempre que aplicável.

Programadores / Analistas – Responsável por participar em todas as fases do processo de desenvolvimento e manutenção de software. Que inclui a análise de requisitos, modelação e arquitetura da solução, implementação da solução, realização de testes e validação dos requisitos, a criação de manuais e documentação de apoio e a formação de utilizadores, sempre que aplicável.

Software Beta Tester – Responsável pela realização de testes e validação dos requisitos.

Analista de Qualidade de Serviço – Responsável pela realização de testes e validação dos requisitos estabelecido, pela criação e revisão dos conteúdos apresentados e realização de auditorias internas ao Gabinete Coordenador de Projetos relativamente às boas praticas de desenvolvimento seguro.

Administrador de Segurança – Responsável global por implementar as políticas e práticas de segurança.

Administrador de Sistemas – Autorizado a instalar, configurar e manter os sistemas.

Operador de Sistemas – Responsável por operar diariamente o sistema do ponto de vista aplicacional. Responsável por operar diariamente os servidores que dão suporte ao sistema aplicacional.

Auditor de Sistemas – Autorizado a monitorizar os arquivos de atividade dos sistemas e registo de eventos para auditoria.

Técnico de Apoio – Prestam assistência e acompanhamento técnico à plataforma.
É da responsabilidade dos Técnicos de Apoio cumprir com os processos e politicas no âmbito dos Sistemas de Gestão.

Técnico de Contabilidade – Responsável pela faturação e controlo de documentos contabilísticos da ACIN.

Técnica Administrativa – Responsável pela execução de diversas tarefas administrativas, necessárias ao bom funcionamento da ACIN.

Gestor do Risco – Responsável pela identificação, avaliação e tratamento de riscos.

Gestor de Capacidade – Responsável por garantir a disponibilidade permanente de todos os recursos necessários à continuidade do negócio.

Gestor de Incidentes de Segurança da Informação – Responsável por assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e pontos fracos de segurança.

Gestor de Criptografia - Responsável pelo desenvolvimento e implementação da Política sobre a utilização de controlos criptográficos.

Gestor de Redes e comunicações - Responsável pela Gestão e controlo das redes de comunicações para proteção da informação.

Gestor de Sistemas Informáticos - Responsável pela Gestão e controlo dos sistemas informáticos.

Gestor de Fornecedores – Responsável por gerir o relacionamento com os fornecedores.
É da responsabilidade do Gestor de Fornecedores, cumprir com os processos e políticas no âmbito do SGSI.

Gestor de Continuidade de Negócio – Responsável por assegurar o funcionamento contínuo da organização e a recuperação atempada da sua atividade.

Gestor de Conformidade das Plataformas Aplicacionais – Responsável por coordenar todos os projetos de desenvolvimento de software.

11. Medidas de segurança da PayPay

10.2. Identificação de Dados Sensíveis de pagamento na PayPay

Tendo em conta o método de pagamento por multibanco, cartões de crédito/débito e MBWAY identificamos como dados de pagamento sensíveis os seguintes:

I. IBAN do cliente
II. Número máximo de Referências Diárias
III. Montante máximo por referência
IV. Montante máximo diário
V. Preçário

10.3. Proteção dos serviços

A PAYPAYUE utiliza o protocolo de segurança 3D Secure. Este protocolo 3D Secure foi desenvolvido pelas principais marcas de Cartão de Crédito/Débito e possibilita a autenticação inequívoca de todos os intervenientes numa transação de comércio eletrónico. Este protocolo é utilizado pela VISA com a designação de Verified By Visa, e pela Mastercard com a designação de Secure Code. Desta forma, quando um cliente realiza um pagamento no portal www.paypay.pt é acionado um processo que verifica se o Cartão de Crédito/Débito utilizado é válido.

Os sistemas de segurança associados ao protocolo 3D Secure, validam a identidade do cliente e informam o portal www.paypay.pt que o cartão utilizado para pagamento é legítimo. Desta maneira, é possível eliminar a fraude e os custos e perdas associados ao tratamento destas situações. Todo este processo decorre de forma automática e perfeitamente transparente. A proteção dada por este protocolo nomeadamente em compras de origem fraudulenta, é totalmente garantida. A PayPay compromete-se a dar resposta a qualquer solicitação que os titulares dos cartões apresentem num prazo máximo de 2 dias.

O portal www.paypay.pt utiliza o protocolo de encriptação de segurança (TSL) para salvaguardar a segurança e confidencialidade dos dados introduzidos pelo utilizador (art.º. 76.º). É perfeitamente seguro inserir os dados do seu Cartão de Crédito/Débito em qualquer pagamento efetuado no www.paypay.pt, uma vez que todos os dados serão inseridos num Servidor Seguro (TSL de 256 bits) que encripta/codifica (transforma num código) todos os dados confidenciais relativos ao seu Cartão de Crédito/Débito.

A PayPayUE – Instituição de Pagamento, Unipessoal, Lda. assegura que não aluga ou vende os dados dos seus clientes a terceiros (art.º. 32.º), pelo que todas as informações são confidenciais e utilizadas apenas pela PayPayUE – Instituição de Pagamento, Unipessoal, Lda. para processamento do pagamento e eventual envio de comunicação que reforce e personalize a oferta cultural ou de produtos.

Diariamente, a PayPay procura promover a melhoria contínua de políticas e procedimentos internos, que permitam prevenir o branqueamento de capitais e do financiamento do terrorismo. Este tipo e atividade concretiza-se através do cumprimento de toda a legislação e regulamentação aplicável, pelo respeito dos princípios éticos e pela adoção das boas práticas internacionalmente aceites, de acordo com o disposto na Lei n.º 25/2008, de 5 de junho.

Os colaboradores da sociedade encontram-se obrigados ao cumprimento rigoroso de todos os deveres consagrados no ordenamento jurídico vigente, designadamente os deveres de exame e de comunicação de todas as operações passíveis de apresentarem risco de BC e/ou FT, constituindo a formação um dos aspetos primordiais de todo o sistema de prevenção.

Para uma verificação e confirmação de viabilidade e veracidade das informações enviadas, antes de ativar as contas dos clientes é solicitado o envio de cópia da documentação de identificação do cliente individual e da empresa a que pertence, de acordo com as diretrizes do Banco de Portugal (entidade que supervisiona as atividades das instituições financeiras, Decreto-Lei n.º 242.2012).

10.4. Garantia de Pagamentos seguros

Sempre que se pretenda alterar, adicionar ou remover um IBAN para receção de fundos, tem que ser realizado pelo representante legal da entidade que está definido na PayPay.
Desta forma, apenas os clientes podem solicitar a alteração de IBAN, excluindo a possibilidade de um colaborador da PayPay alterar a conta erroneamente, ou mesmo propositadamente, mitigando a possibilidade de fraude.

O pedido é realizado diretamente em www.paypay.com, uma vez realizada a autenticação pelo cliente. Sempre que exista um pedido de alteração ou adição de novo IBAN é enviado um alerta por e-mail ao Compliance. O envio do comprovativo de IBAN deve ser enviado pelo representante legal da empresa que solicitou na plataforma este pedido, para garantir à PayPay que:

- Foi efetivamente o representante legal que solicitou o pedido de alteração do IBAN;
- Que o IBAN registado pertence à entidade.

Após uma confirmação escrita, o Compliance aprova o IBAN, anexando o comprovativo na ficha do cliente na plataforma.

Em função do procedimento estipulado pela PayPay o cliente pode apenas solicitar a alteração, não consegue de forma alguma modificar efetivamente o IBAN diretamente na plataforma, pois requer validação obrigatória por parte da PayPay.

10.5. Controlo de clientes de elevado risco

Sempre que a PayPay recebe do Banco de Portugal a informação de um cliente a ser considerado de elevado risco, a PayPay regista na plataforma esta informação, por forma a que, caso um cliente desta lista faça o registo, a plataforma emite um alerta na ficha do cliente por aprovar e bloqueia a a possibilidade de aprovação deste cliente.

Caso se trata de um cliente que já esteja registado e a utilizar a PayPay, ao inserir os dados como Cliente de elevado risco a plataforma emite um alerta para o Compliance, para que este possa informar o cliente e inativar os acessos na PayPay.

10.6. Monitorização e medição de operações

A Monitorização e medição das operações de controlo da PayPay, é realizada através dos seguintes indicadores:

I. Valor mensal recebido superior à média mensal do cliente;
II. Valor mensal recebido inferior à média mensal do cliente;
III. Recebimentos por referência;
IV. Número de recebimentos por mês.

10.5.1. Emissão de notificações

A plataforma envia alertas ao Compliance, por e-mail e para o TOC, na sua ausência, sempre que existam indicadores de suspeição de operações relacionadas com o BC/FT previamente definidos na plataforma, nomeadamente:

V. Aumento superior a 40% dos valores recebidos, num determinado mês;
VI. Valor recebido inferior a 40 % da média mensal;
VII. Transações ocasionais de valor igual ou superior a 3.000,00€;
VIII. Receção de 300 ou mais pagamentos mensais numa entidade, salvo exceções que estejam previstas no perfil do cliente.

Sempre que seja detetado um dos indicadores supramencionados, deve o compliance da PayPay comunica estes dados à entidade supervisora das Instituições de pagamento.

12. Gestão do Risco

Com o objetivo de assegurar prontidão e conformidade do sistema de controlo interno, a PAYPAY assume o compromisso de identificar, analisar, qualificar e tratar o risco decorrente de várias fontes de ameaças para os seus compromissos.
A Política de Gestão de Riscos de BC/FT define a metodologia adotada para tratamento dos riscos assim identificados, sendo baseada nas melhores práticas definidas em normas internacionais de referência, e constitui-se como uma ferramenta de gestão da empresa.

11.1. Identificação dos principais riscos

Tendo em conta que se trata de uma plataforma totalmente web, alojada e desenvolvida utilizando a *Cloud Computing* como paradigma de funcionamento, foram identificados um conjunto de cenários genéricos que podem ter impacto na atividade da PAYPAYUE, nomeadamente:

- Falha nos Sistemas de Informação;
- Absentismo dos Colaboradores;
- Falha na Segurança da Informação e/ou Atos Maliciosos;
- Falha nos fornecedores de cadeia de valor;

- Falha ou indisponibilidade da estrutura física / Desastres Naturais (incêndios, anomalias meteorológicas);

Na ocorrência de um destes incidentes o primeiro objetivo será sempre o salvaguardar a integridade física dos colaboradores da PAYPAYUE, e rapidamente a restauração total do normal funcionamento dos serviços.

11.2. Análise do impacto no negócio

Após a ocorrência de um evento, é necessário avaliar os danos provocados pela situação anómala. As seguintes áreas devem ser endereçadas:

- Causa da situação anómala;
- Área da PayPay afetada;
- Estado da infraestrutura física (condição dos sistemas de alimentação de energia elétrica);
- Condição de funcionamento da infraestrutura tecnológica da PayPay (equipamento IT e de comunicações);
- Potencial da situação para provocar perdas ou danos adicionais;
- Tempo estimado para recuperação das condições normais de funcionamento.

Todas as situações não mencionadas carecem de uma análise do Compliance.

Os resultados da avaliação dos danos e seu impacto na organização devem ser confrontados com os critérios de ativação do Plano de Continuidade de Serviços são:

Tipologia	Descrição do critério
Edifício	Indisponibilidade de acesso físico ao edifício ou evacuação do edifício
	O edifício sede da PayPay não garante a segurança necessária à habitabilidade do mesmo
Legal	Investigação regulatória formal ou inquérito.
	Qualquer incidente que possa afetar a capacidade de cumprir com as nossas obrigações legais ou regulamentares e / ou que possam ter impacto sobre a nossa licença como operador.
Perda de Dados / Violação de dados	Qualquer evento que põe em risco a marca ou reputação da organização em resultado de uma séria perda de dados e / ou acesso não autorizado às nossos redes ou sistemas.
Nível de indisponibilidade de serviço	A extensão dos danos infringidos à infraestrutura tecnológica da PayPay provocou uma interrupção no funcionamento do equipamento IT ou de comunicações que suportam os serviços mais críticos e se prevê que esta interrupção seja superior ao tempo máximo admissível para a sua reparação.

11.3. Avaliação do Impacto

Os riscos provenientes das falhas que possam surgir têm probabilidades, no geral, baixas de acontecerem, mas os impactos negativos provenientes dos mesmos podem colocar em causa o desenvolvimento da atividade da empresa total ou parcialmente, por um período longo, caso não sejam implementadas medidas preventivas.
Todos os riscos e ameaças têm recursos afetos diferentes o que promove uma avaliação diferente, em função do que determinado risco possa afetar. A tabela infra é uma média dos valores de cada um dos riscos, retirados da Matriz de Análise de Risco (DS07)

Processo de Avaliação de Riscos				
Identificação dos Riscos	**Análise de Riscos**			**Tempos de Resposta**
	Probabilidade	**Consequência**	**Nível de Risco**	
Falha nos Sistemas de Informação	C	3	III	R.T.O. < 4h
Absentismo dos Colaboradores	C	1	V	R.T.O. < 4h
Falha na Segurança da Informação e/ou Atos Maliciosos	B	3	III	R.P.O. < 24h R.T.O. < 4h
Falha nos fornecedores de cadeia de valor	B	3	III	R.T.O. < 4h
Falha ou indisponibilidade da estrutura física	B	2	III	R.P.O. < 24h R.T.O. < 4h M.A.O. < 48h
Desastres Naturais (incêndios, anomalias meteorológicas)	B	4	II	R.T.O. < 4h

Nível de risco

Nível	Prioridade	Ações de mitigação
I (Muito Alto)	1 (máxima)	É obrigatório o risco já estar tratado ou estar em execução pelo menos uma MTR.
II (Alto)	2	É obrigatório que pelo menos uma MTR esteja planeada para execução antes da revisão do sistema pela gestão.
III (Médio)	3	Será atribuída a responsabilidade de monitorização sistemática ao dono do risco, e de notificação imediata ao Compliance de todas as situações que possam fazer elevar o nível do risco.
IV (Baixo)	4	Será realizada pelo Compliance comunicação aos donos do risco da sua existência e da necessidade de os monitorizar a intervalos regulares.
V (Muito Baixo)	5 (mínima)	Será realizada pelo Compliance comunicação aos donos do risco e da necessidade de rever o seu estado pelo menos uma vez por ano.

11.4. Plano de mitigação dos principais riscos

a) **Falha nos Sistemas de Informação -** Em casos de indisponibilidade de serviço causado por falha do datacenter/infraestrutura técnica de suporte ao sistema, a empresa garante a existência de redundância dos elementos críticos da plataforma proposta, entre outros, base de dados, alimentação elétrica, comunicações; garante o backup diário da base de dados; tem disponibilidade global da solução de 99,8% e disponibilidade específica nas horas úteis das 9h às 19h de 99,9 %; garante um centro alternativo para recuperação em caso de desastre, com ativação num prazo de 72 horas; e garante a monitorização e operação da solução 24x7x365, com tempo de intervenção técnica no local de alojamento inferior a 2 horas.
Na falha ou indisponibilidade causada por operacionalização de nova versão é realizado um backup total antes do processo de atualização. Caso seja identificada alguma inconformidade o sistema é reposto usando a script de atualização. Este processo demora no máximo 60 minutos.
A PAYPAYUE fica alojada no Data Center da ONI, em Máquinas Virtuais, que tem os seus servidores distribuídos por três locais. No caso de haver um desastre total do Data Center em que está alojada a aplicação, e a aplicação ficar indisponível, é feito um telefonema ao suporte ONI. Se após esse telefonema se confirmar que houve um desastre no Data Center então é dada a ordem, pela gerência, para que a ONI reponha os backups do dia anterior a funcionar num dos outros dois Data Centers. Os DNS's e redireccionamentos também são alterados por eles de modo a apontar para a nova localização.

b) **Absentismo dos Colaboradores -** Na eventualidade de haver um surto de gripe ou equivalente que reduza ou ameace infetar grande parte dos recursos humanos será atribuído acessos remotos via VPN aos colaboradores e estes, visto todos terem acesso à Internet, poderão se ligar aos escritórios da empresa e continuar a desempenhar as suas funções. Poderá inclusive ser atribuído telefones VoIP pré configurados para poderem continuar a receber e fazer chamadas através dos escritórios da PayPay.

c) **Falha na Segurança da Informação e/ou Atos Maliciosos** - A empresa assegura a qualidade da informação, precavendo o acesso a informações por pessoas não autorizadas e evitando que os dados sejam alterados ou apagados sem permissão, através da criação de acessos individuais.

d) **Falha ou indisponibilidade da estrutura física / Desastres Naturais (incêndios, anomalias meteorológicas)** - No caso de falhas na infraestrutura ou na ocorrência de desastres naturais (incêndios, terremotos, cheias) e os escritórios ficarem destruídos, a base de operações passa para a casa privada da gestão da empresa, situada na Rua 6 de Maio, nº 11. A casa está provida de Internet e tem espaço para acomodar pelo menos os colaboradores com funções mais críticas para manter a empresa a funcionar. Fica a menos de 3 minutos a pé das instalações atuais da ACIN, o que permite coordenar as operações de reconstrução/recuperação dos escritórios.

13. Gestão de Incidentes e Gestão da Continuidade de Negócio

Todos os eventos que coloquem em causa os compromissos de segurança da informação e a atividade da PayPay serão tratados como possíveis incidentes e como tal inseridos no processo de gestão de incidentes da PayPay.
O respetivo diagnóstico de causas, consequências, medidas de controlo e mitigação do risco decorrentes serão tratadas segundo as melhores práticas, estando previsto a ativação de processos disciplinares e ações judiciais para matérias que enquadrem dolo ou violação de responsabilidades assumidas por terceiras partes.
A disponibilidade da informação, não descurando a responsabilidade dos restantes compromissos de segurança da informação, será assegurada pela implementação de respostas a incidentes disruptivos e que se integram no âmbito do Processo de Continuidade de Negócio da PAYPAY.

14. Formação e sensibilização

A sensibilização, treino e formação sistemática dos colaboradores da PAYPAY em matérias de segurança da informação, branqueamento de capitais e/ou financiamento do terrorismo é uma forte aposta decorrente do compromisso da empresa.

15. Divulgação e publicação

A divulgação da formalização das decisões da Liderança da PayPay é assegurada através de uma Política de Comunicação.

A publicação interna de documentos relevantes para a operacionalização da segurança da informação é considerada essencial para que os colaboradores da empresa se sintam corresponsáveis e que cumpram e façam cumprir as determinações definidas neste sentido.