POLÍTICA DE CONTINUIDADE DE NEGÓCIOS ("PCN")

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.

LÍDER DO CONGLOMERADO PRUDENCIAL

Validade e Atualização

Esta Política é válida pelo prazo de 2 (dois) ano a partir da data da última revisão constante na tabela ao final, devendo ser revisada e atualizada antes do fim da validade, nas hipóteses de alteração da legislação aplicável e/ou de direcionamento estratégico do conglomerado prudencial do PagSeguro Internet Instituição de Pagamento S.A.

1. INTRODUÇÃO E OBJETIVO

1. Introdução

A presente **Política de Continuidade de Negócios** ("PCN" ou "Política") do **PagSeguro Internet Instituição de Pagamento S.A.** ("PagSeguro"), instituição líder do Conglomerado Prudencial, do **BancoSeguro S.A.** ("BancoSeguro") **PagInvest Corretora de Títulos e Valores Ltda.**(PagInvest CTVM) e **Wirecard Brazil Instituição de Pagamento S.A** (MOIP), instituições pertencentes ao conglomerado prudencial do PagSeguro e em conjunto denominadas ("Companhias"), foi elaborada com base na legislação em vigor e nas normas editadas pelo Banco Central do Brasil ("BACEN") e outros entes regulatórios, bem como nas melhores práticas de mercado.

A partir dos conceitos, princípios e diretrizes estabelecidos nesta Política, as Companhias fortalecem a estrutura de gerenciamento de riscos e a governança corporativa em Continuidade de Negócios, oferecendo mais segurança aos seus profissionais, clientes e acionistas diante de imprevistos, bem como busca assegurar um nível adequado de estabilidade organizacional nos momentos posteriores a eventuais interrupções e durante todo o processo de recuperação.

1.2 Objetivo

Os objetivos foram definidos para suportar e manter a segurança dos processos de negócio das Companhias, garantindo que sejam retornados a sua condição operacional normal em um prazo aceitável, por ocasião da ocorrência de um incidente . Estes objetivos são medidos por meio dos indicadores e monitoramentos:

- % da eficiência dos Planos de Continuidade de Negócios, constatando possíveis impactos internos que possam comprometer a continuidade das Companhias;
- % de testes de Carga realizados no ano para identificarmos o limite de capacidade do sistema e qual o limitante (hardware, tempo de resposta excessivo, throughput);
- % Exercícios de DR e Mesa para os sitemas bem como, a aplicação de exercícios para preservar a vida dos profissionais e dos prestadores de serviços, identificando possíveis ameaças e impactos internos e externos que possam comprometer a continuidade das Companhias;
- % Treinamentos de Capacitações para os profissionais e prestadores de serviços na trilha documental obrigatória de GCN;
- Monitoramento das ações de melhoria continua e adequação do sistema de gestão da continuidade do negócio das Companhias.
- Monitoramento dos documentos de continuidade de negócios, afim de garantir que as informações permanem atualizadas e disponíveis.

2. ABRANGÊNCIA

Esta Política é aplicável a todo público interno, processos e áreas das Companhias, independentemente da estruturação em unidades físicas ou virtuais e/ou forma de acesso, se local ou remoto, ao ambiente das Companhias.

Em trando-se das demais partes interessadas : Clientes Pessoa Física (PF) e Pessoa Jurídica(PJ), está Política é aplicável no tocante ao atendimento de suas necessidades e expectativas a qual as Companhias desenvolvem meios eficientes para processar as operações de negócio de maneira segura em um nível aceitável de capacidade predefinido durante uma disrupção.

2.1 Escopo

Assegurar a retomada em tempo hábil e em um nível aceitável das atividades críticas do negócio:

- Soluções de pagamentos para o comércio eletrônico, atendendo lojas virtuais, e também para estabelecimentos comerciais,
- Viabilizar concessões de crédito, investimentos e outros produtos e serviços importantes para o dia a dia de seus clientes., e
- Plataforma de investimento online da conta digital PagBank que compreende : investimentos em CDBs, Fundos de Investimento , Renda Variável e Tesouro Direto.
- Sistema de pagamentos para lojas físicas e virtuais.

Em caso de interrupção por falhas ou desastres significativos, aplicáveis aos sistemas críticos classificados em P1(crise) e P 2(indisponibilidade) localizados nos Data Centers Glete, Tamboré e ambientes de cloud pública como por exemplo: AWS, OCI etc. bem como, aos processos de negócio classificados em altos e críticos localizados nas estruturas físicas nos endereços: Avenida Brigadeiro Faria Lima, 1384/ 1485 e Avenida Barão de Limeira, 426/428, garantindo planos de continuidade que sejam capazes de responder efetivamente a uma disrupção.

2.2 Regras

A Continuidade de Negócios é um processo abrangente, que identifica ameaças potenciais inerentes aos negócios das Companhias e os possíveis impactos nas operações provenientes de tais ameaças. Fornece uma estrutura para que se desenvolva um nível de resiliência organizacional que seja capaz de responder efetivamente e proteger os interesses das partes envolvidas, a reputação, as marcas das Companhias e suas atividades de valor agregado.

A Continuidade de Negócios contempla o gerenciamento da recuperação em caso de interrupção e gestão de todo o Programa de Continuidade por meio de treinamentos, planos, testes, revisões e manutenções, a fim de garantir sua operacionalização e atualização.

3. DEFINIÇÃO

Acordo de Nível de Operacional (ANO): acordo entre um provedor de serviço de TI (Tecnologia da Informação) e outra parte interessada. Dá apoio na entrega dos serviços de TI a clientes definindo os produtos, condições ou serviços a serem fornecidos e as respectivas responsabilidades entre as partes.

Acordo de Nível de Serviço (ANS): acordo definitivo firmado entre áreas das Companhias e os fornecedores, descrevendo serviços, metas de nível de serviço, além de papéis e responsabilidades das partes envolvidas no acordo.

Análise de Impacto do Negócio (*Business Impact Analysis* - *BIA*): processo de analisar o impacto de uma disrupção na organização ao longo do tempo.

Atividade: conjunto de uma ou mais tarefas com uma saída definida.

Atividades prioritárias: atividades, cuja urgência é determinada de forma a evitar impactos inaceitáveis aos negócios, durante uma disrupção.

Auditoria: processo sistemático, independente e documentado para obtenção de evidência de auditoria e avaliá-la objetivamente para determinar a extensão na qual os critérios de auditoria são atendidos.

***Backup*:** cópia de segurança de dados de um dispositivo para um outro local ou mídia de armazenamento que possa ser restaurada em caso de perda acidental ou de corrupção dos dados no dispositivo original.

Comitê de Segurança da Informação e Governança de Dados: órgão permanente, com poder institucional, que monitora, instaura regras e delibera sobre os interesses, dentre outros assuntos, sobre o contexto de continuidade nas Companhias.

Continuidade de Negócios: capacidade de uma organização continuar a entrega de produtos ou serviços em um nível aceitável com capacidade predefinida durante uma disrupção.

Competência: capacidade de aplicar conhecimento e habilidades para alcançar resultados pretendidos.

Desastres de Grande Porte: inundações, alagamentos, enchentes, incêndios, desmoronamentos, sinistros, terrorismo, pandemias, ou ainda qualquer outra situação não prevista nessa Política, que gere impacto na continuidade das atividades das Companhias.

***Disaster Recovery* (DR):** processo que inclui um ou mais conjuntos de procedimentos e planos responsáveis pela recuperação de serviços após um evento extremo.

Disrupção: Incidente, seja previsto ou imprevisto, que causa um desvio não planejado e negativo da expectativa de entrega de produtos e serviços de acordo com os objetivos da organização.

GCN: Gestão da Continuidade do Negócio.

Incidente: evento que pode representar ou levar á disrupção de negócios, perdas, emergências ou crises.

ITR: Instrução de Trabalho.

Instrução CVM Nº 555, de 17 de dezembro de 2014, com as alterações introduzida pelas instruções CVM Nº 563/15, 564/15, 572/15, 582/16, 587/17, 604/18, 605/19, 606/19, 615/19 e Resolução CVM Nº 3/20: dispõe sobre a constituição, a administração, o funcionamento e a divulgação de informações dos fundos de investimentos.

Instrução de Trabalho GCN.ITR.004: tem por objetivo garantir a sistemática que será adotada quanto a utilização da Sala de Resposta a Incidentes.

Instrução de Trabalho GCN.ITR.005: assegurar o registro e tratamento de Incidentes, garantir a normalização da operação e/ou serviço afetado o mais rápido possível dentro da estrutura da CIA .

Melhoria Contínua: atividade recorrente para elevar o desempenho Norma NBR ISO 22301/2020: norma base para o Sistema de Gestão de Continuidade de Negócios – Requisitos.

Mídia: mecanismos em que dados podem ser armazenados além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas, papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos, que são diferentes tipos de mídia.

Objetivo Mínimo de Continuidade de Negócios: níveis mínimos aceitáveis de serviços e/ou produtos para as Companhias alcançarem seus objetivos de negócios durante uma interrupção.

Partes interresadas: *stakeholder* (termo admitido) pessoa ou *organização* que pode afetar, ser afetado ou que entende ser afetado por uma decisão ou *atividade por exemplo:* EXEMPLO: Clientes, proprietários, funcionários, fornecedores, banqueiros, reguladores, sindicatos, parceiros ou sociedade, podendo incluir concorrentes ou grupos de interes ses opostos.

PCO – Plano de Continuidade Operacional: composto por procedimentos previamente definidos, destinados a manter a continuidade operacional dos serviços vitais da organização na ocorrência de anormalidades.

PGI – Plano de Gerenciamento de Incidente: plano orientado às respostas aos incidentes que vierem a ocorrer no centro operações. Considera o incidente ocorrido, estrutura, atuação e a comunicação por meio dos canais da empresa.

PRD – Plano de Recuperação de Desastres: baseado na importância e sensibilidade dos ativos, define o planejamento da restauração, ações relativas à convocação dos recursos para atender situações de crise, procedimentos de recuperação de ambientes ou movimentação para sites de redundância.

PTV - Plano de Testes e Validações: são testes regulares do Grupo Gestor de Continuidade que, em conjunto com outras áreas das Companhias, estrutura e realiza testes, corrigindo irregularidades dos planos e submetendo-os ao conhecimento dos gestores, para que estes promovam melhorias e adequações constantes.

Plano de Continuidade de Negócios: informação documentada que orienta a organização a responder a uma disrupção e retomar , recuperar e restaurar a entrega de produtos e serviços de acordo com os objetivos de continuidade de negócios.

Política: intenções e direções de uma organização, como formalmente expressos pela sua Alta Direção.

Política de Backup: estabelecer as diretrizes aos procedimentos de backup, para minimizar a possibilidade de perda ou danos os dados, bem como a viabilização de sua recuperação em caso de incidentes que tenham origens por meio de ações voluntárias ou acidentais.

Processo: conjunto de atividades inter-relacionadas ou interativas que transformam entradas em saídas.

Profissional: todo e qualquer empregado, diretor estatutário, estagiário, ou terceiro das Companhias e de áreas do Grupo UOL que as atendem.

Resiliência: refere-se à capacidade das Companhias de retomarem suas atividades normais após um evento de interrupção em seus negócios.

Resolução CVM nº 35/21: estabelece normas e procedimentos a serem observados nas operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários.

Resolução nº 4.502, de 30 de junho de 2016: estabelece requisitos mínimos a serem observados na elaboração e na execução de planos de recuperação por instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Resolução nº 4.557, de 23 de fevereiro de 2017: dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital.

Restore: processo de restauração do dado copiado, de volta a um estágio desejado em uma área acessível.

Risco: a probabilidade de insucesso de um determinado evento acontecer, gerando possíveis perdas.

RTO - Objetivo do Tempo de Recuperação (*Recovery Time Objective*): período para retomar uma atividade ou processo crítico após sua interrupção. É o "tempo alvo para recuperação de um sistema, ambiente ou aplicação de TI após um incidente". RTO define o tempo que as Companhias conseguem conviver com a ausência dessa atividade sem grandes impactos. Tem como delimitadores a decretação do regime de contingência e o retorno da execução da atividade.

RPO - Objetivo do Ponto de Recuperação (*Recovery Point Objective*): posição (ponto) na qual deverão estar disponíveis os dados das aplicações recuperáveis após a ocorrência de um desastre. O ponto em que a informação usada por uma atividade deve ser restaurada para permitir a operação da atividade retomada. É o último instante de tempo em que os dados de um sistema computacional se encontravam íntegros e armazenados de alguma maneira, estando disponíveis para serem utilizados em um processo de recuperação.

Sistema Crítico: serviço de informação considerado essencial para uma função crítica do negócio, podendo envolver *hardware*, *software*, pessoas e processos necessários para garantir a viabilidade ou a continuidade das operações.

Site de Contingência: os processos críticos das Companhias quando acionados a contingência são realizadas em home office. No que tange ao Data Center possuímos Sites redundantes onde os sistemas críticos rodam em Glete e AWS e sua contingência encontra-se em Tamboré, podendo ser utilizado como ativo-ativo, ou ativo standby conforme necessidade, características ou limitação de cada aplicação.

Suspensão de Atividades: interrupção das atividades por alterações nas regras dos órgãos regulatórios e fiscais, por inadimplência de bandeiras ou por conflito de ordem política.

4. PAPÉIS E RESPONSABILIDADES

Todos os profissionais notadamente dentro de suas correspondentes atividades têm funções e responsabilidade relacionadas a Gestão de Continuidade de Negócios. As posições adiante apontadas são identificadas como tendo funções e responsabilidades diretas pelo Programa:

4.1 Segurança da Informação (Gestão da Continuidade do Negócios- GCN)

a) Analisar o resultado dos testes de Disaster Recovery (DR) dos fornecedores críticos para as Companhias, estabelecidos nos Acordos de Níveis de Serviços (ANS) e propor melhorias;
b) Apoiar a construção de checklist de testes de *Disaster Recovery* (DR) para os diversos times e unidades de negócio, bem como a metodologia para execução deles em conjunto com os responsáveis e pontos focais pelos Planos de Continuidade de Negócios;
c) Consolidar os resultados dos exercícios dos Planos de Continuidade de Negócios e Disaster Recovery por meio da elaboração de relatórios periódicos, reportando-os ao Comitê de Segurança da Informação e Governança de Dados e à Diretoria;
d) Cumprir o disposto nos documentos de Continuidade de Negócios;
e) Definir a metodologia e ferramentas a serem utilizadas para condução da Gestão de Continuidade de Negócios, orquestrando o Programa como um todo;
f) Implementar anualmente o processo de Análises de Impacto(BIA) nas Companhias;
g) Propor projetos e iniciativas para o aperfeiçoamento da Gestão de Continuidade de Negócios das Companhias, buscando alinhamento às melhores práticas existentes;
h) Realizar análises crítica e atualizações regulares das análises de impacto (BIA) e de análises de riscos e considerar possíveis oportunidades de melhoria contínua do desempenho e relevância ao programa de continuidade de negócios e desta política;
i) Desenvolver as capacitações da trilha documental obrigatória de GCN, bem como, os treinamentos de GCN da Plataforma UniUOL ;
j) Recepcionar os impactos significativos da Diretoria para elaboração dos BIAs;
k) Reportar à Diretoria os resultados dos testes documentados e avaliados no Comitê de Segurança da Informação e Governança de Dados, permitindo o aprimoramento contínuo dos procedimentos, do gerenciamento de riscos e da recuperação;
l) Reportar aos órgãos reguladores, agências e entidades de acompanhamento, sempre que necessário, informações atualizadas e fidedignas sobre esse Programa.

4.2 Profissionais

a) Buscar orientação junto à área de Segurança da Informação com o time de Gestão da Continuidade do Negócio em caso de dúvidas relacionadas ao GCN, às Normas e a Continuidade de Negócios;
b) Cumprir o disposto nos documentos de Continuidade de Negócios;
c) Participar ativamente dos processos de teste e planejamento, sempre que requisitados; e
d) Realizar as capacitações da trilha documental obrigatória de GCN, bem como, os treinamentos de GCN da Plataforma UniUOL.

4.3 Gestores

a) Acionar e seguir a Instrução de Trabalho (GCN.ITR.004) sempre que necessário;
b) Acionar e seguir a Instrução de Trabalho (GCN.ITR.005) sempre que necessário;
c) Na ocorrência de evento que tenha provocado o acionamento do Plano de Continuidade de Negócios , deve ser comunicado à Compliance ;
d) Cumprir o disposto nos documentos de Continuidade de Negócios;

e) Garantir a participação ativa dos profissionais sob sua gestão nos processos que compreendem a elaboração, bem como participação nos Planos de Continuidade de Negócios;
f) Identificar e indicar um profissional responsável para representar a gestão da continuidade de negócios pelos seus documentos;
g) Participar e indicar profissionais para participação dos exercícios e testes validando ao longo do tempo a eficiencia e a validade das suas estrategiaas e soluções de continudiade de negócios;
h) Participar no desenvolvimento da Análise de Impato (BIA) com intuito de analisar o impacto nos negócios e avaliar os riscos de disrupção;e
i) Realizar as capacitações da trilha documental obrigatória de GCN, bem como, os treinamentos de GCN da Plataforma UniUOl.

4.4 Comunicação

Em caso de desastre de grande porte ou suspensão de atividades, a área de Comunicação das Companhias deverá comunicar seus clientes e , acionistas por meio de canais e times apropriados a respeito de tais situações, levando sempre em consideração o parecer da área Juridica que compreende os aspectos legais, judiciais e extrajudiciais das Companhias, estas ações estão relacionadas ao Plano de Administração de Crise o qual é tratado por meio da GCN.ITR.004 - Metodologia para utilização Sala de Resposta a Incidentes.

4.5 Risco e Compliance

a) Analisar a Política de Continuidade de Negócios garantindo que a mesma esteja apropriada aos objetivos de continuidade de negócios das Companhias;
b) Comunicar os incidentes relevantes que afetem os sistemas críticos e que tenham impacto significativo sobre os clientes, comunicar tempestivamente os órgãos de administração e a SMI, após a materialização do incidente, informando aos órgãos reguladores, conforme especificado na Resolução CVM 35;
c) Disponibilizar a Política (resumo) para as partes interessadas por meio da página das Companhias;
d) Solicitar a disponibilização da Politica de Continuidade de Negócios na intranet das Companhias para os profissionais; e
e) Solicitar aprovação da Política de Continuidade de Negócios aos patrocinadores pela mesma, tendo seu registro por meio de ata.

4.6 CRO PagSeguro Pagbank e CFO PagSeguro Pagbank

a) O CRO e CFO são patrocinadores desta Política, sendo responsável por assegurar que o programa receba suporte adequado.
b) A responsabilidade efetiva pelo cumprimento das disposições desta Política cabe ao gestor das respectivas áreas. Ainda, é de competência dos referidos determinar as diretrizes institucionais com base em valores e princípios estabelecidos na presente política, nas normas de controles internos, nas normas emanadas dos órgãos e entidades de regulação e autorregulação e nas melhores práticas aplicáveis.

5. DIRETRIZES

São diretrizes do programa de Continuidade de Negócios:

a) Aprimorar a qualidade e efetividade das estratégias, planos e processos estabelecidos para a continuidade de seus negócios, investino em metodologias que atendam os padrões para a perenidade de seus negócios considerando as necessidades e expectativas das partes interessadas.

b) Estabelecer os objetivos, metas, controles, processos e procedimentos relevantes para melhorar a Continuidade de Negócio e obter resultados alinhados com as políticas e objetivos estratégicos das Companhias, O monitoramento dos resultados e atingimento dos objetivos são medidos e comunicados para a alta direção por meio Análise crítica;

c) Identificar e garantir a aplicação dos requisitos legais e regulatórios para as Companhias previstos nas instruções, regulamentações, dentre outros;

d) Realizar exercícios e testes anuais para validar a eficiência e a validade das suas estratégias e solucções de continuidade de negócios por meio de exercícios de mesa e simulações de desastre que garantam a manutenção da continuidade, bem como o funcionamento dos planos de continuidade (PCO, PAC, PRD, PGI, PTV e PRD). Os resultados dos exercícios e testes são documentados permitindo o aprimoramento contínuo do gerenciamento de riscos e recuperação;

e) Revisar anualmente ou a partir de mudanças relevantes (podem decorrer de atualizações, migrações, implantação de novos produtos, novas demandas, entre outras modificações informadas pelas unidades de negócios para que o impacto apurado em cada processo permaneça condizente com a realidade do negócio) de toda a documentação pertinente a Gestão de Continuidade de Negócios;

f) Analisar o impacto da interrupção das atividades das Companhias ao longo do tempo, determinar os seus tempos de recuperação e identificar as atividades críticas e recuperá-las em um nível e tempo aceitáveis;

g) Assegurar que todos os profissionais compreendam suas responsabilidades perante a Continuidade de Negócios, por meio da realização de treinamentos e conscientização sobre o tema;

h) Desenvolver estrutura de gerenciamento e resposta a crises, suportada por níveis adequados de autoridade e competência, que assegurem a comunicação efetiva às partes interessadas;

i) Estabelecer papéis e responsabilidades das partes internas e externas às Companhias;

j) Identificar e avaliar os terceiros que exercem função crítica na cadeia de valor e colaboração do processo de negócio;

k) Assegurar a revisão periódica do desempenho do Sistema de Gestão de Continuidade de Negócio e a implementação de ações corretivas e de melhoria;

l) Adotar práticas de mitigação de risco adequadas à dimensão das ameaças e à extensão de seus possíveis impactos;

m) Estabelecer a identificação de práticas para retomada de serviços e mitigação do risco operacional em processo formal de análise de impacto no negócio; e

n) Preservar a integridade física das pessoas por meio de Planos e exercícios e testes garantindo o bem estar dos profissionais.

6. DÚVIDAS

Dúvidas sobre esta Política devem ser encaminhadas à área de Segurança da Informação, pelo e-mail l-pagseguro-dresden-continuidade@uolinc.com.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

O conteúdo desta Política é classificado, de acordo com a Política de Classificação da Informação, como Informação Interna.

8. CONSIDERAÇÕES FINAIS

Essa Política foi aprovada pela Diretoria do PagSeguro, em reunião realizada em 10 de abril de 2023.

9. ANEXOS

N/A.

10. CONTROLE DE ALTERAÇÕES

Revisão	Alterações	Data
00	Emissão inicial | Segurança da Informação & *Compliance*	Janeiro/2019
01	Primeira versão | Segurança da Informação & *Compliance*	Março/2020
02	Segunda versão | Segurança da Informação & *Compliance*	Dezembro/2020
03	Terceira versão | Segurança da Informação & *Compliance*	Março/2022
04	Quarta versão | Segurança da Informação & *Compliance*	Abril/2023

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A. – SEGURANÇA DA INFORMAÇÃO & COMPLIANCE