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) anos 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 PagSeguro Internet Instituição de Pagamento S.A.; BancoSeguro S.A. e PagInvest S.A.

Sumário

1. INTRODUÇÃO E OBJETIVO

1.1. Introdução

A presente **Política de Continuidade de Negócios** ("PCN" ou "Política") é aplicável ao **PagSeguro Internet Instituição de Pagamento S.A**. ("PagBank"), instituição líder do Conglomerado Prudencial, do **BancoSeguro S.A.** ("BancoSeguro"), **WireCard Brazil Instituição de Pagamentos S.A** ("MOIP"), **PagInvest Corretora de Títulos e Valores Mobiliários LTDA** ("PagInvest"), em conjunto denominadas "Companhias". Tendo em vista que as disposições da presente política se aplicam a todas as empresas integrantes do Conglomerado Prudencial, tais disposições, também, se estendem ao Fundo de Investimento em Direitos Creditórios PagSeguro I ("FIDC PagSeguro")[1] e Fundo de Investimento em Direitos Creditórios – PagBank Multiadquirência – Responsabilidade Limitada ("FIDC Multiadquirência", sendo em conjunto com FIDC PagSeguro, "FIDCs")[1], ao PagSeguro Biva Securitizadora de Créditos Financeiros S.A. ("Biva")[1]." , 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 da Companhia, 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:

- 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 sistemas 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;

[1] Tendo em vista que os FIDCs são representados pela sua administradora e não pelos seus cotistas e a "Biva" é uma securitizadora, a aplicabilidade das disposições dessa Política se dá por serem integrantes do Conglomerado Prudencial.

- Monitoramento das ações de melhoria contínua e adequação do sistema de gestão da continuidade do negócio das Companhias;
- Monitoramento dos documentos de continuidade de negócios, a fim de garantir que as informações permanecem atualizadas e disponíveis;
- Monitoramento ao atendimento de chamados (jira) do sistema de gestão de continuidade de negócios garantindo que os profissionais tenham acesso eficiente aos documentos de continuidade;
- % de Não Conformidades por auditoria internas e externas da ISO 22301, esse indicador avalia a intensidade e a frequência das não conformidades nas auditorias, permitindo identificar tendências e áreas críticas, além de orientar ações corretivas e melhorias contínuas;
- Taxa de Cumprimento de SLA (*Service Level Agreement*) permitindo avaliar a eficácia da CIA em cumprir os tempos de resposta e os parâmetros de qualidade estabelecidos no SLA, tanto em situações normais quanto em crises;
- % de engajamento dos gestores em estratégias de continuidade de negócio, garantindo que as ações e decisões de continuidade de negócios sejam bem integradas nas metas estratégicas da CIA que seus planos estejam atualizados e revisados e aptos quando acionados;
- % de compensação das emissões de Gases de Efeito Estufa (GEE): Tornar-se uma empresa neutra em carbono nos escopos 1, 2 e 3.
- Selo Ouro do Programa Brasileiro GHC *Protocol*: Garantir a publicação de Inventários de Gases de Efeito Estufa completos e verificados por terceira parte independente.
- Disponibilidade do Sistema (em %) durante o período de monitoramento: Calcular o tempo em que o sistema esteve funcionando (*uptime*) em comparação ao tempo total possível de funcionamento (tempo total de monitoramento).

2. REGULAMENTAÇÃO

Resolução nº 4.557/17 - Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

Resolução nº 4.656/18 - Dispõe sobre a sociedade de crédito direto e a sociedade de empréstimo entre pessoas, disciplina a realização de operações de empréstimo e de financiamento entre pessoas por meio de plataforma eletrônica e estabelece os requisitos e os procedimentos para autorização para funcionamento, transferência de controle societário, reorganização societária e cancelamento da autorização dessas instituições.

ISO 22301:2020 - Este documento especifica os requisitos para implementar, manter e melhorar um sistema de gestão para proteger-se, reduzir a probabilidade de ocorrência, preparar-se, responder a e recuperar-se de disrupções quando estas ocorrerem.

ISO 22313:2020 - Este documento fornece orientações e recomendações para a aplicação dos requisitos do sistema de gestão de continuidade de negócios (SGCN) fornecidos na ABNT NBR ISO 22301. As orientações e recomendações são baseadas em boas práticas internacionais.

CVM nº 35/21 - Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários

Resolução BCB n° 131/21 - Consolida as normas sobre o rito do processo administrativo sancionador, a aplicação de penalidades, o termo de compromisso, as medidas acautelatórias, a multa cominatória e o acordo administrativo em processo de supervisão, previstos na Lei nº 13.506, de 13 de novembro de 2017, e os parâmetros para a aplicação das penalidades administrativas previstas na Lei nº 9.613, de 3 de março de 1998.

Resolução CMN n° 4.893/21 - Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

Resolução BCB n° 232/22 - Estabelece os procedimentos para o reconhecimento de instrumentos mitigadores no cálculo da parcela dos ativos ponderados pelo risco (RWA) referente às exposições ao risco de crédito sujeitas ao cálculo do requerimento de capital mediante abordagem padronizada (RWA_{CPAD}).

Resolução BCB nº 265/22 - Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de instituição classificada como Tipo 3 enquadrada no Segmento 2 – S2, Segmento 3 – S3 ou Segmento 4 – S4.

Resolução CVM 175/22 - Dispõe sobre a constituição, o funcionamento e a divulgação de informações dos fundos de investimento, bem como sobre a prestação de serviços para os fundos, e revoga as normas que especifica.

Resolução CMN n° 5.187/24 - Dispõe sobre o processo de planejamento da recuperação e da resolução de instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

ISO 22301:2024 – Esta emenda é uma adoção idêntica no conteúdo técnico estrutura e redação da "emenda de Ação Climática! Às Normas de Sistema de Gestão (MSS) ABNT NBR ISO existentes e novas, para refletir os compromissos de ação climática da ISO .

3. 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 tratando-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 a Companhia desenvolve meios eficientes para processar as operações de negócio de maneira segura em um nível aceitável de capacidade predefinido durante uma disrupção.

3.1. Escopo

Os planos de continuidade de negócios estabelecem procedimentos e prazos para reinício e recuperação das atividades, assegurando 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 para estabelecimentos comerciais;
- Viabilizar concessões de crédito, investimentos e outros produtos e serviços importantes para o dia a dia de seus clientes;
- 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; e
- Oferta de serviços relacionados a compra, venda, troca de moedas estrangeiras, transferências e remessas internacionais.

Os prazos são declarados em cada plano, conforme a criticidade de cada processo, bem como as comunicações necessárias, sejam internas ou externas e detalham o processo que deve ser adotado antes, durante e após a situação de contingência.
O processo de análise de impacto no negócio inclui a avaliação, identificação, classificação e o impacto nos processos críticos, resultando que, em caso de interrupção por falhas ou desastres significativos, aplicáveis aos sistemas críticos classificados em P1(crise) e P2(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 ,425 garantindo planos de continuidade que sejam capazes de responder efetivamente a uma disrupção.
Para o tratamento e os procedimentos dos incidentes relacionados a ambiente cibernético, processamento e armazenamento de dados e de computação em nuvem contratados, são tratados em instrução de trabalho específica, abrange todos os cenários.

3.2. Regras

A Continuidade de Negócios é um processo abrangente, que identifica ameaças 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.

4. 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*): análise de consequência processo (3.1.190) de análise de todas as funções operacionais e dos efeitos que uma interrupção operacional pode ter sobre elas.

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 Interna: (3.1.14) conduzida por uma organização (3.1.165), ou em nome dela, para gestão (3.1.144) análise Crítica (3.1.211) ou outro propósito interno, a qual pode compor a base da autodeclaração de conformidade (3.1.44) da organização.

***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.

Circular nº 3.877 de 30 de novembro de 2017 (Banco Central do Brasil) **– requisitos de segurança para instituições financeiras e de pagamento.**

Circular nº 3.910 de 25 de setembro de 2018 (Banco Central do Brasil) **– regras sobre instituições de pagamento e sistemas de pagamentos, incluindo gestão de riscos e continuidade dos serviços.**

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.

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

Continuidade: capacidade estratégica e tática, pré-aprovada pela gestão (3.1.144), de uma organização (3.1.165) par planejar e responder a condições, situações e eventos (3.1.96) a fim de continuar as operações em um nível predefinido aceitável.

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.

Diretiva NIS2 (Diretiva da União Europeia sobre Segurança de Redes e Sistemas de Informação) – para organizações na União Europeia, essa diretiva estabelece requisitos para a segurança de redes e sistemas de informação, que inclui aspectos da continuidade de negócios.

***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 (3.1.122), antecipado ou imprevisto, que resulta em desvios negativos e não planejados na entrega esperada de produtos e serviços (3.1.191) de acordo com os objetivos (3.1.162) da organização (3.1.165).
GCN: Gestão da Continuidade do Negócio.
Incidente: evento (3.1.96) que pode consistir ou poderia levar a uma disrupção (3.1.75), perdas, emergência (3.1.87) ou crise (3.1.60)
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.
ITR: Instrução de Trabalho.
Lei *Sarbanes-Oxley* (SOX) – nos Estados Unidos, essa lei exige que empresas públicas estabeleçam controles internos e procedimentos para garantir a integridade das informações financeiras, o que pode impactar a continuidade dos negócios.
Melhoria Contínua: atividade (3.1.2) recorrente para aumentar o desempenho (3.1.177).
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 (MBCO): capacidade (3.1.25) mínima ou nível de serviços e/ou produtos que é aceitável para uma organização (3.1.165) para atingir seus objetivos (3.1.162) de negócios durante uma disrupção (3.1.75).
Partes interessadas: *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 interesse opostos.
PCI DSS (*Payment Card Industry Data Security Standard*) – este padrão estabelece requisitos para a proteção de dados de cartões de pagamento e inclui aspectos relacionados à continuidade dos negócios, especialmente na proteção e segurança das informações financeiras.
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.

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 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.

Política: intenções e direção de uma organização (3.1.165), como formalmente expresso pela sua Alta Direção (3.1.279).

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.

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.

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.

Resiliência Organizacional: capacidade de uma organização (3.1.165) em observar e se adaptar em um ambiente de mudanças.

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.

Resolução nº 4.656 de 26 de abril de 2018 (Banco Central do Brasil) – esta resolução trata do gerenciamento de riscos operacionais e incluem diretrizes para a continuidade de negócios e a resiliência das operações.

Resolução nº 4.657 de 26 de abril de 2018 (Banco Central do Brasil) **– diretrizes para governança e gestão de riscos em instituições financeiras.**

Resolução nº 4.658 de 26 de abril de 2018 (Banco Central do Brasil) – estabelece normas para a gestão de riscos em instituições financeiras, incluindo a gestão de continuidade de negócios.

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

Requisito: necessidade ou expectativa que é declarada, geralmente implícita ou obrigatória.

Recurso: todos os ativos (3.1.13) (incluindo instalações e equipamentos), pessoas, habilidades, tecnologia, instalações, e suprimentos e informação (3.1.127) (eletrônicas ou não) que uma organização (3.1.165) deve ter disponível para usarem quando necessário, a fim de operar e cumprir seu objetivo (3.1.162).

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

RPO - Objetivo do Ponto de Recuperação (*Recovery Point Objective*): ponto para o qual a informação (3.1.127) usada por uma atividade (3.1.2) é restaurada para permitir que a atividade de operação seja retomada.

RTO - Objetivo do Tempo de Recuperação (*Recovery Time Objective*): período após um incidente (3.1.122) dentro do qual um produto e serviço (3.1.191) ou uma atividade (3.1.2) é retomada, ou os recursos (3.1.207) estão recuperados.

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 da Companhia 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.

Organização: pessoa ou grupo de pessoas com suas próprias funções, com responsabilidade, autoridades e relações para alcançar seus objetivos (3.1.162).

5. 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:

5.1. 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, bianualmente, o processo de Análise de Impacto (BIA) na empresa para os processos críticos, e realizar essa análise para os demais processos a cada três anos;
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 para os escopos certificados 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 das 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; e
l) Reportar aos órgãos reguladores, agências e entidades de acompanhamento, sempre que necessário, informações atualizadas e fidedignas sobre esse Programa.

5.2. Profissionais

a) Buscar orientação junto à área de Segurança da Informação com o time de Gestão da Continuidade do Negócio (GCN) em caso de dúvidas relacionadas ao Sistema de Gestão da 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.

5.3. Gestores

a) Acionar e seguir a Instrução de Trabalho (GCN.ITR.004 - Metodologia para utilização da *War Room* a Incidentes e Administração de Crise - PAC) sempre que necessário;

b) Acionar e seguir a Instrução de Trabalho (GCN.ITR.005 - Metodologia para registro e tratamento dos Incidentes do PagSeguro) 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 eficiência e a validade das suas estratégias e soluções de continuidade de negócios;
h) Participar no desenvolvimento da Análise de Impacto (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.

5.4. 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 Jurídica que compreende os aspectos legais, judiciais e extrajudiciais da Companhia, 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.

5.5. Risco e Compliance

a) Analisar a Política de Continuidade de Negócios garantindo que ela esteja apropriada aos objetivos de continuidade de negócios da Companhia;
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 para as partes interessadas por meio da página da Companhia (podendo essa ser resumida ou na integra);
d) Solicitar a disponibilização da Política de Continuidade de Negócios na intranet da Companhia para os profissionais; e
e) Solicitar aprovação da Política de Continuidade de Negócios aos patrocinadores pela mesma, tendo seu registro por meio de ata.

5.6. 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.

6. DIRETRIZES

São diretrizes do programa de Continuidade de Negócios:

a) Aprimorar a qualidade e efetividade das estratégias, planos e processos estabelecidos para a continuidade dos negócios, investindo em metodologias que atendam aos padrões de resiliência, considerando não apenas as necessidades e expectativas das partes interessadas, mas também os impactos das mudanças climáticas e desastres ambientais;

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 de 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 efetividade das estratégias e soluções 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 testes servem para revisar e monitorar a eficiência e eficácia dos planos, e 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, lições apreendidas com as mudanças climáticas, atualizações de regulamentações ambientais 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, considerando os riscos ambientais e os efeitos das mudanças climáticas no tempo de recuperação de operações críticas. A análise deve identificar e priorizar as atividades essenciais que, caso interrompidas, teriam impacto direto nas operações ou no meio ambiente, e definir planos para recuperá-las em níveis aceitáveis e dentro de um tempo adequado;

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 uma estrutura de gerenciamento e resposta a crises, suportada por níveis adequados de autoridade e competência, que assegure uma comunicação efetiva com todas as partes interessadas, inclusive durante crises climáticas e desastres naturais;

i) Estabelecer papéis e responsabilidades das partes internas e externas à companhia, garantindo que os fornecedores e parceiros críticos também adotem práticas de continuidade;

j) Assegurar a revisão periódica do desempenho do Sistema de Gestão de Continuidade de Negócio bem como a adoção de práticas de melhoria contínua, visando a adaptação a mudanças internas e externas e o fortalecimento da resiliência organizacional;

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

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

m) Preservar a integridade física das pessoas, por meio de planos e exercícios que garantam o bem-estar dos profissionais.

7. DÚVIDAS

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

8. CLASSIFICAÇÃO DA INFORMAÇÃO

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

9. CONSIDERAÇÕES FINAIS

Essa Política foi aprovada pela Diretoria do PagSeguro, em reunião realizada em 18 de julho de 2025.

10. ANEXOS

N/A.

11. CONTROLE DE ALTERAÇÕES

Revisão	Alterações	Data
00	Emissão Companhia | 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
05	Quinta versão | Segurança da Informação & *Compliance*	Junho/2025

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