POLÍTICA DE CONTINUIDADE DE NEGÓCIOS ("PCN")

WIRECARD BRAZIL S.A.

1 VALIDADE E ATUALIZAÇÃO

Esta Política é válida pelo prazo de 1 (um) 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 da Wirecard Brazil S.A.

Date	Autor	Sumário de modificações
23/02/2022	Segurança da Informação	Emissão inicial

Vigência: fevereiro/2022
Versão: 0

2 INTRODUÇÃO E OBJETIVO

A presente **Política de Continuidade de Negócios** ("PCN" ou "Política") da **Wirecard Brazil S.A.** ("Wirecard" ou "Companhia"), 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, a Companhia fortalece a estrutura de gerenciamento de riscos e a governança corporativa em Continuidade de Negócios, oferecendo mais segurança aos seus profissionais e clientes 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.

3 ABRANGÊNCIA

Esta Política é aplicável a todos os profissionais, processos e áreas da Companhia, independentemente da estruturação em unidades físicas ou virtuais e/ou forma de acesso, se local ou remoto, ao ambiente da Companhia.

3.1 ESCOPO

Assegurar a retomada em tempo hábil e em um nível aceitável das atividades críticas do negócio, em caso de interrupção por falhas ou desastres significativos, aplicáveis aos sistemas críticos e processos de negócios, localizados nas estruturas físicas da Companhia.

3.2 REGRAS

A Continuidade de Negócios é um processo abrangente, que identifica ameaças potenciais inerentes aos negócios da Companhia 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 da Companhia 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 DEFINIÇÕES

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 da Companhia 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.

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 da Companhia.

***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 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.

Norma NBR ISO 22301/2020: norma base para o Sistema de Gestão de Continuidade de Negócios – Requisitos.

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.

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 da Cia., 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 om s objetivos de continuidade de negócios.

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

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

Profissional: todo e qualquer empregado, diretor estatutário, estagiário, ou terceiro da Companhia.

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

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.
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.

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 DE NEGÓCIOS)

a) Analisar o resultado dos testes de DR dos fornecedores críticos para as Companhias, estabelecidos nos Acordos de Níveis de Serviços (ANS) e propor melhorias;
b) Consolidar os resultados de testes e exercícios dos Planos de Continuidade de Negócios por meio da elaboração de relatórios periódicos, reportando-os ao Comitê de Segurança da Informação e Governança de Dados e à Diretoria;
c) Cumprir o disposto nos documentos de Continuidade de Negócios;
d) Definir a metodologia e ferramentas a serem utilizadas para condução da Gestão de Continuidade de Negócios, orquestrando o Programa como um todo;
e) Apoiar a construção de checklist de testes de Disaster Recovery (DR) para os diversos times e torres, bem como a metodologia para execução deles em conjunto com os responsáveis e pontos focais pelos Planos de Continuidade de Negócios;
f) Propor projetos e iniciativas para o aperfeiçoamento da Gestão de Continuidade de Negócios da Companhia, buscando alinhamento às melhores práticas existentes;
g) Recepcionar os impactos significativos da Diretoria para elaboração dos BIAs;
h) 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
i) 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 em caso de dúvidas relacionadas ao GCN, às Normas e a Continuidade de Negócios;
b) Cumprir o disposto nos documentos de Continuidade de Negócios; e
c) Participar ativamente dos processos de teste e planejamento, sempre que requisitados.

5.3 GERENTES

a) Cumprir o disposto nos documentos de Continuidade de Negócios;

b) Garantir a participação ativa dos profissionais sob sua gestão nos processos que compreendem a elaboração, bem como participação nos Planos de Continuidade de Negócios;
c) Realizar os treinamentos obrigatórios;
d) Acionar e seguir a Instrução de Trabalho (GCN.ITR.004) sempre que necessário; e
e) Acionar e seguir a Instrução de Trabalho (GCN.ITR.005) sempre que necessário

5.4 COMUNICAÇÕES

Em caso de desastre de grande porte ou suspensão de atividades, a área de Comunicação da Companhia deverá comunicar seus clientes e acionistas por meio de canais e times apropriados a respeito de tais situações.

5.5 DIRETORIA

A Diretoria é patrocinadora desta Política, sendo responsável por assegurar que o programa receba suporte adequado. A responsabilidade efetiva pelo cumprimento das disposições desta Política cabe ao gestor das respectivas áreas. Ainda, é de competência dos referidos Diretores 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) 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 da Companhia;
b) Identificar e garantir a aplicação dos requisitos legais e regulatórios para as Companhias previstos nas instruções, regulamentações, dentre outros;
c) Realizar testes anuais de mesa e simulações de desastre que garantam a manutenção da continuidade, bem como o funcionamento dos planos de continuidade (PCO, PAC , PGI, PTV e PRD);
d) Revisão anual (ou a partir de mudança relevante) de toda a documentação pertinente a Gestão de Continuidade de Negócios;
e) Analisar o impacto da interrupção das atividades da Companhia ao longo do tempo, determinar os seus tempos de recuperação e identificar as atividades críticas e recuperá-las em um nível e tempo aceitáveis;
f) Assegurar que todos os profissionais compreendam suas responsabilidades perante a Continuidade de Negócios, por meio da realização de treinamentos e conscientização sobre o tema;
g) Desenvolver estrutura de gerenciamento e resposta a crises, suportada por níveis adequados de autoridade e competência, que assegurem a comunicação efetiva às partes interessadas;
h) Estabelecer papéis e responsabilidades das partes internas e externas às Companhias;
i) Identificar e avaliar os terceiros que exercem função crítica na cadeia de valor e colaboração do processo de negócio;
j) Assegurar a revisão periódica do desempenho do Sistema de Gestão de Continuidade de Negócio e a implementação de ações corretivas e de melhoria;
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.

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 da *Wirecard* em reunião realizada em xx de fevereiro de 2022.