

GRC-POL-003 - Política do Sistema de Gestão de Continuidade de Negócios



POLÍTICA DO SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS	GRC-POL - 003
	Data Publicação: 03/2026

Classificação da Informação: ☒Pública ☐Interna ☐Restrita ☐Confidencial

Sumário

1. OBJETIVO
2. ABRANGÊNCIA
3. NORMAS E CERTIFICAÇÕES
4. DOCUMENTOS DE REFERÊNCIA
5. DISPOSIÇÕES GERAIS
6. DIRETRIZES
7. RESPONSABILIDADES
8. DEFINIÇÕES
9. CONTROLE DE REVISÕES

1.OBJETIVO

A presente Política do Sistema de Gestão de Continuidade de Negócios (“Política”) tem por objetivo estabelecer as diretrizes do Sistema de Gestão de Continuidade de Negócios (“SGCN”), visando contribuir para a resiliência e a sustentabilidade dos negócios antes, durante e depois de situações de crise através do planejamento, implantação e adoção de Planos de Continuidade de Negócios (“PCNs”) e afins para uso em situações de crise previamente definidas e avaliadas pela organização.

2.ABRANGÊNCIA

Esta política é aplicável às empresas Dock Instituição de Pagamento S.A (Dock IP), Dock Soluções em Meios de Pagamento S.A, (Dock Soluções) Dock Tecnologia S.A (Dock Tech), Ônix Serviços de Valor Agregado S.A (Ônix), bem como as demais unidades de negócios em que a Dock atua constituídas no Brasil. Neste documento as empresas mencionadas serão denominadas Grupo Dock.

3.NORMAS E CERTIFICAÇÕES

☒ BACEN

☐ PCI

☐ SOX

☒ ISO 27.001

☒ ISO 27.701

☒ ISO 22.301

☒ ISO 31.000

☒ LEI PARA REGULAMENTAR AS INSTITUIÇÕES DE TECNOLOGIA FINANCEIRA (MÉXICO)

☐ NENHUMA DAS NORMAS

4.DOCUMENTOS DE REFERÊNCIA

GRC-NOR-001 - Gestão de Normativos;

GRC-POL-022 - Gerenciamento de Crises;

SI-POL-001 - Política de Segurança da Informação e Cibernética

GRC-POL-022 -Gestão de Crises

IA-MAN-001 - Manual Operacional de Auditoria Interna

GRC-MAN-003-Manual do Sistema de Gestão de Continuidade de Negócios

5.DISPOSIÇÕES GERAIS

Os colaboradores envolvidos no processo em questão estão cientes de que as diretrizes definidas neste documento poderão ser auditadas. Portanto, recomenda-se não salvar cópias

dos normativos na área de trabalho/diretórios da rede ou imprimi-los. O colaborador deve sempre acessar a ferramenta Confluence.

6.DIRETRIZES

O Sistema de Gestão de Continuidade de Negócios (SGCN) é um elemento estratégico de governança corporativa integrado aos demais sistemas de gestão da organização. Para implementação e manutenção deste, o grupo Dock deve considerar:

- A identificação, avaliação e consideração de questões internas e externas relevantes na elaboração dos procedimentos associados ao SGCN;
- A identificação das partes interessadas e de seus respectivos requisitos;
- A observância e avaliação dos requisitos legais e regulatórios aplicáveis à elaboração e implementação do SGCN;
- A definição e formalização de papéis e responsabilidades para as áreas envolvidas no programa de continuidade de negócios;
- A definição e declaração do escopo do Sistema de Gestão de Continuidade de Negócios;
- A adoção de práticas voltadas à melhoria contínua do programa;
- A adoção de medidas para preservação da integridade física das pessoas;
- A implementação de ações de educação, treinamento, conscientização e comunicação, assegurando que os colaboradores compreendam suas responsabilidades no âmbito da continuidade de negócios;
- O estabelecimento e o monitoramento de indicadores para acompanhamento de continuidade de negócios.

6.1. Análise de Impacto ao Negócio (BIA)

O Grupo Dock deve realizar a Análise de Impacto ao Negócio a fim de identificar, analisar e priorizar processos críticos, bem como os impactos decorrentes de sua interrupção. Desta forma, aplicam-se as seguintes diretrizes:

- Deve ser realizada a definição de uma matriz de impacto, considerando critérios de impacto claros e proporcionais ao seu contexto, assim como níveis que permitam a identificação e priorização de processos críticos;
- Dependências internas e externas relevantes para a continuidade dos negócios devem ser consideradas;
- Devem ser estabelecidos objetivos de tempo de recuperação (RTO) e objetivos de Ponto de Recuperação (RPO), a fim de minimizar os impactos.

- Recursos essenciais para a execução dos processos críticos devem ser identificados e mapeados, incluindo pessoas, tecnologia, informações, instalações e fornecedores;

Os resultados da Análise de Impacto de Negócios(BIA) devem definir o escopo abrangido pelo Plano de Continuidade de Negócios e demais procedimentos, assim como exclusões e justificativas.

Uma análise de riscos deve ser realizada a fim de identificar e avaliar possíveis cenários que podem ocasionar disrupções nos processos críticos identificados pelo BIA.

6.2 Processo de Gestão de Crises (PGC)

Um processo de gestão de crises deve ser implementado de forma que:

- Sejam definidos critérios de crise para ativação do Plano de Continuidade de Negócios;
- Ações de antes, durante e depois da crise devem ser implementadas;
- Fluxos de comunicação de acordo com a linha do tempo de crise sejam estabelecidos;
- Pessoas-chave para a execução da estratégia sejam envolvidas.

6.3. Plano de Continuidade de Negócios (PCN)

O Plano de Continuidade de Negócios é composto por um conjunto de procedimentos interdependentes que se integram e se acionam de forma coordenada. O PCN deve:

- Atuar como instrumento orientador e centralizador, direcionando o acionamento dos demais planos quando aplicável;
- Descrever a estratégia de continuidade de negócios;
- Abranger os processos e cenários identificados pela Análise de Impacto ao Negócio (BIA);
- Assegurar a integração com o processo de gestão de crises;

6.3.1. Plano de Continuidade Operacional (PCO)

O Plano de Continuidade Operacional (PCO) deve contemplar ações que assegurem a manutenção e/ou retomada das atividades operacionais críticas em frente aos cenários de disrupção identificados. De forma que:

- Deve contemplar estratégias de continuidade, levando em consideração cenários de emergência e contingenciamento do processo abrangido;
- Devem ser considerados recursos essenciais, dependências externas e internas e fornecedores relevantes;
- Ativos e ferramentas essenciais para continuidade devem ser contemplados;
- Pessoas-chave, fornecedores e terceiros relevantes devem ser identificados, assim como suas ações nas estratégias dos planos;

- Deve detalhar alternativas operacionais para a manutenção das atividades críticas.

6.3.2. Plano de Recuperação de Desastres

- Deve ser orientado pelo resultado da Análise de Impacto ao negócio (BIA);
- Deve contemplar a recuperação dos sistemas, dados e serviços essenciais ao negócio;
- Deve assegurar a disponibilidade, confidencialidade e integridade das informações.

6.4. Programa de Exercícios

Para assegurar a eficiência das atividades contempladas pelo Plano de Continuidade de Negócios e seus procedimentos associados, o Grupo Dock deve:

- Estabelecer um programa de exercícios periódicos;
- Documentar e analisar os resultados dos exercícios realizados;

Em caso de situações extraordinárias um novo prazo para a realização dos exercícios, diferente da periodicidade estabelecida, pode ser definido através de análise crítica.

6.5. Lições Aprendidas

Convém que lições aprendidas sejam documentadas quando o Plano de Continuidade de Negócios for acionado ou quando houverem desvios nos exercícios.

6.6 Treinamento e Conscientização

Para assegurar a efetividade do SGCN e o correto entendimento dos papéis e responsabilidades, o grupo Dock deve:

- Promover ações periódicas de treinamentos;
- Garantir com que o nível de capacitação dos colaboradores envolvidos seja compatível com as responsabilidades atribuídas;
- Assegurar que a conscientização alcance as partes envolvidas;

6.7 Análise Crítica

O Sistema de Gestão de Continuidade de Negócios deve passar periodicamente por Análise crítica, com o intuito de avaliar sua adequação, suficiência e eficácia.

6.8 Auditorias Internas

As auditorias internas devem ocorrer periodicamente. Os auditores internos (próprios ou terceirizados) devem comprovar qualificação e competência nos requisitos da Norma a ser auditada.

A seleção de auditores e a condução da auditoria devem garantir a objetividade e

imparcialidade exigidas pelo SGCN. Por isso, um programa de auditorias internas é estabelecido no IA-MAN-001 - MANUAL OPERACIONAL DE AUDITORIA INTERNA

7.RESPONSABILIDADES

Todos os colaboradores têm responsabilidades, considerando as atividades correspondentes a sua área, em assegurar a aplicação das diretrizes estabelecidas nesta política.

7.1 Alta Direção e Comitê de Segurança (Estratégico)

Papel: Patrocínio, Apetite ao Risco e Resposta ao Regulador.

- **Aprovação:** Validar estratégias de GCN e definir o apetite ao risco da Dock.
- **Recursos:** Garantir orçamento e pessoal para a resiliência organizacional.
- **Governança:** Realizar a análise crítica do desempenho do sistema e deliberar sobre indicadores.
- **Regulatório:** Representar a Dock perante o **Banco Central do Brasil** e outros órgãos.

7.2 Área de Continuidade de Negócios (Tático/Gestão)

Papel: Guardiã da Metodologia e Orquestradora do SGCN.

- **Metodologia:** Coordenar o SGCN, realizando o **BIA** e identificando ativos críticos.
- **Apoio Técnico:** Orientar a criação de planos (PCN, PRD, Contingência) e melhorias contínuas.
- **Validação:** Gerir métricas, validar resultados de testes e reportar ao Comitê.
- **Cultura:** Promover treinamentos e alinhar o calendário anual de exercícios simulados.

7.3 Diretoria de Tecnologia e Operações (Gestão Operacional / Execução)

Papel: Autoridade de Aprovação Técnica e Operacional.

- **Aprovação Técnica:** Validar os BIAs, PCNs e PRDs sob sua gestão.
- **Execução:** Assegurar o armazenamento de informações críticas e o cumprimento de prazos de testes.
- **Alinhamento:** Definir, junto à Continuidade, o escopo e as datas das janelas de teste.
- **Resiliência:** Garantir a disponibilidade da infraestrutura e estratégias de recuperação (Backup, DR).
- **Documentação:** Construir os planos técnicos (PRD) e preencher os dados do BIA.
- **Prática:** Executar testes, produzir relatórios de avaliação e participar de simulações.

7.4 Segurança da Informação, Gestão de Riscos e Fornecedores (Execução, Suporte e Conformidade)

Papel: Monitoramento e Extensão da Resiliência.

- **Segurança da Informação:** Mitigar riscos cibernéticos e atuar no contingenciamento de incidentes de segurança.
- **Riscos:** Avaliar e monitorar riscos de continuidade conforme a política de GRC.
- **Terceiros:** Garantir que fornecedores críticos atendam aos requisitos de continuidade e participem de testes quando aplicável.

8.DEFINIÇÕES

SGCN : Sistema de Gestão de Continuidade de Negócios

PCN(Planos de Continuidade de Negócios): Conjunto de documentos estruturados que relacionam as atividades necessárias para a recuperação de um processo crítico, redução dos impactos causados por uma interrupção e o adequado nível de comunicação a ser exercido durante o processo de recuperação;

PCO(Plano de continuidade Operacional): descreve as alternativas para a execução de procedimentos ordenados, normalmente operacionais/manuais, que têm como objetivo manter o processo/serviço funcionando sem impactar no cliente.

PRD (Plano de Recuperação de Desastres): considerando a criticidade dos ativos, é definido o planejamento da recuperação, ações relativas à convocação dos recursos para atender situações de crise, procedimentos de recuperação de ambientes ou movimentação para sites e/ou infra estruturas redundantes.

PGC(Plano de Gerenciamento de Crise): estabelece papéis, responsabilidades e as diretrizes para a Gestão de Crise, buscando direcionar a estratégia de contingência a ser adotada pela Dock durante a ocorrência ou a ameaça de crise, até que sejam restabelecidas as condições normais.

PCOM(Plano de Comunicação): A comunicação na crise é de suma importância para todas as partes, por isso o plano de comunicação prevê comunicação adequada às partes interessadas, antecipando o passo a passo dessa gestão no caso de uma situação sensível.

BIA (Business Impact Analysis/Análise de impacto no negócio): A análise de impacto no negócio é um processo que analisa os processos de negócios relacionando os impactos qualitativos e quantitativos em caso de interrupção destes, proporcionando uma visão executiva sobre os processos mais impactantes para a Companhia.

RTO – Recovery Time Objective ou Objetivo de tempo de recuperação (OTR): Limite de tempo definido para ativação de Continuidade ou recuperação.

RPO – Recovery Point Objective ou Ponto Objetivo de Recuperação (POR): Está relacionado à quantidade de dados que a empresa tolera perder no caso de um desastre.

9.CONTROLE DE REVISÕES

Esse normativo passa a vigorar a partir de sua publicação e deve ser revisado sempre que fatos alterarem o disposto neste documento ou anualmente.

Este documento será revisto e atualizado quando:

- Houver solicitação de atendimento, correção ou adição de informações;
- Existir a necessidade de atender requisitos legais, boas práticas ou recomendações de auditoria;
- Existir mudança na organização que tenha impacto relevante na atividade abordada neste documento;
- No vencimento de 12 meses a contar da publicação.

Revisão n°	Descrição da Revisão	Revisor	Gerente	Executivo
0.0	Elaboração do documento	William Evaristo	Renata Ravelli	Thiago Cunha
1.0	Revisão anual da política	Jefferson Campos	Renata Ravelli	Thiago Cunha
1.1	Inclusão de normativos e leis no item 3	Jefferson Campos	Renata Ravelli	Thiago Cunha
2.0	Inclusão e correções no item 9 - Estratégia de Continuidade de Negócios	Jefferson Campos	Renata Ravelli	Thiago Cunha
3.0	Revisão anual política	Camila Silveira	Renata Ravelli	Thiago Cunha
4.0	Item 6.8 definição de medição de indicadores e item 6.9 Auditorias internas	Camila Silveira	Renata Ravelli	Thiago Cunha

5.0	Ajuste item 4.Documentos De Referência do nome do manual GRC-MAN-003 - Manual de Gestão de Continuidade	Camila Silveira	Renata Ravelli	Thiago Cunha
6.0	Revisão anual política 2025 (responsabilidades, estratégia)	Nilma Raposo	Tatiane Paya	Thiago Cunha
7.0	Revisão anual política 2026 (classificação, normativo auditoria	Stephanny Nascimento/ Nilma Raposo	Tatiane Paya	Thiago Cunha