Warren Rena

POLÍTICA DE GESTÃO CONTINUIDADE DE NEGÓCIOS

06/2025

Classificação
Política

Título
Gestão de Continuidade de Negócios

Versão
06

Data de atualização
23/06/2025

.

1. OBJETIVO

Este documento tem como objetivo dotar a Instituição de recursos que permitam manter a continuidade operacional dos seus processos críticos em situações de excepcionalidade, bem como identificar os fatores de risco que possam comprometer a continuidade dos negócios, apresentando alternativas com custo inferior e proporcional ao da possível perda operacional. Objetiva, também, conscientizar os colaboradores a manterem-se alertas a possíveis riscos de descontinuidade operacional e estarem aptos e treinados no tocante à utilização de recursos alternativos em situações de contingência; em conformidade com o determinado pela Diretoria Executiva de TI e Diretoria de Compliance, Controles Internos e Auditoria, pelas normas e legislações vigentes.

2. APLICAÇÃO

As regras estabelecidas neste documento devem ser cumpridas pelos dirigentes, colaboradores, prestadores de serviços (“Colaboradores” / “Colaborador”) e parceiros externos vinculados ao Grupo Warren.

3. BASE REGULATÓRIA

Resolução CVM nº 35, de 26 de maio de 2021: Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

Resolução CMN Nº 4.968, de 25 de novembro de 2021: Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

4. DIRETRIZES GERAIS

O Plano de Continuidade de Negócios é um conjunto de estratégias, procedimentos e informações documentadas que orientam a organização na preparação, resposta e recuperação diante de eventos que possam causar interrupções significativas em suas atividades. Seu objetivo é garantir que os processos críticos possam ser mantidos ou restabelecidos dentro de prazos aceitáveis, reduzindo impactos operacionais, financeiros, legais e reputacionais.

O Plano de Continuidade de Negócios (PCN) deve ser desenvolvido preventivamente, com base em estratégias e planos táticos que garantam a resiliência operacional da organização.

A Warren Rena estruturou seu PCN com base em um planejamento que contempla os seguintes elementos:

4.1. Identificação e classificação de processos críticos

A Warren Rena utiliza internamente um Formulário Eletrônico de Business Impact Analysis (BIA), com o objetivo de mapear e analisar processos e atividades de negócio. Essa análise considera os impactos da indisponibilidade de cada processo e permite a priorização das ações de recuperação com base na criticidade.

Através do referido formulário, são avaliados os riscos associados à indisponibilidade de recursos essenciais, incluindo pessoas, sistemas, infraestrutura e fornecedores, permitindo a definição de ações de mitigação apropriadas, bem como a identificação e classificação de processos críticos, possibilitando a definição de prioridades de recuperação, tempos máximos de retomada e os recursos mínimos necessários (humanos, tecnológicos e estruturais).

4.2. Desenvolvimento do Plano de Continuidade de Negócios

Com os processos críticos devidamente mapeados e priorizados, é elaborado o Plano de Continuidade de Negócios, contendo estratégias de resposta, procedimentos de recuperação, rotinas de backup e responsabilidades definidas.

Portanto, o PCN refere-se aos processos que deverão ser observados em cenários de incidentes relevantes ou emergências. O PCN será formalizado no documento “Plano de Continuidade Operacional (PCO)”.

4.3. Teste de Efetividade

Anualmente, deverão ser realizados testes a fim de avaliar a efetividade e a funcionalidade do Plano de Continuidade do Negócio. Os resultados deverão ser formalizado em relatório, deverá observar:

- Consolidar os resultados dos testes realizados;
- Cumprir o disposto no PCN;
- Diante dos resultados, propor iniciativas de aperfeiçoamento do PCN;
- Reportar à Diretoria os resultados dos testes documentados e avaliados, permitindo o
- aprimoramento contínuo dos procedimentos, do gerenciamento de riscos e da recuperação.
-

A Gerência de Segurança da Informação deve preencher o relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. É imprescindível a apresentação do respectivo relatório, à Diretoria Executiva, até 31 de março do ano seguinte ao da data-base.

4.4. Treinamento e Conscientização

Para garantir a efetividade do processo de Gestão de Continuidade do Negócio, devem ser realizados workshops de conscientização e treinamentos que assegurem que os colaboradores estejam cientes de suas responsabilidades e preparados para agir diante de eventuais interrupções que venham a ocorrer.

4.5. Gestão de Incidentes

A gestão de incidentes na Warren Rena tem como objetivo detectar, responder e recuperar eventos que possam comprometer a continuidade dos serviços, a integridade das informações ou a segurança operacional da instituição. Este processo envolve ações coordenadas, registros adequados e uma abordagem estruturada para mitigar impactos e prevenir recorrências.

Os registros dos incidentes serão realizados através de Sistema Interno, para que uma análise e categorização do incidente seja realizada.

Cada incidente deverá ser classificado de acordo com seu grau de gravidade/relevância.

Os cenários que possuírem uma das seguintes características deverão ser considerados como relevantes:

- Incidentes que acionarem o PCN;
- Envolverem Processos Críticos e acionarem o PCN;
- Incidentes de segurança cibernética relevantes os que afetam os processos críticos de negócios, dados ou informações sensíveis que tenham impacto significativo sobre os clientes;

Após, os incidentes serão classificados, os seguintes processos serão executados:

- Investigação
- Diagnóstico
- Resolução e Recuperação
- Conclusão
- Para os incidentes considerados, inicialmente relevantes, será avaliado a necessidade do acionamento do PCN e Plano de Comunicação.

4.6. Processos Críticos

Processos críticos são processos e atividades operacionais cuja interrupção ou indisponibilidade não programados podem provocar impacto negativo significativo nos negócios do intermediário

Serão considerados processos críticos no mínimo aqueles que abrangeram os seguintes processos:

I – recepção e execução de ordens, com o objetivo de preservar o atendimento aos clientes;

II – liquidação junto às entidades administradoras de mercados organizados;

III – liquidação de seus clientes; e

IV – conciliação e atualização das posições de seus clientes.

4.7. Comunicação

(i) Comunicado ao Banco Central

Incidentes relevantes que configurem situação de crise serão comunicaçãos ao Banco Central do Brasil no prazo máximo de 72 horas após a identificação.

A área de Compliance é responsável pela elaboração e envio desta comunicação.

Todo incidente que acionar o PCN será considerado situação de crise.

(ii) Comunicado à Superintendência de Relações com o Mercado e Intermediários (SMI) e alta administração

Ocorrências que acionarem o Plano de Continuidade de Negócios devem ser comunicadas à Superintendência de Relações com o Mercado e Intermediários (SMI), bem como à Alta Administração, no prazo máximo de 72 horas após a identificação.

O comunicado deve conter, no mínimo:

- causas do acionamento do plano de continuidade de negócios, indicando os processos críticos afetados;
- medidas já adotadas pelo intermediário ou as que pretende adotar;
- tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e
- qualquer outra informação considerada importante.

A área de Compliance é responsável pela elaboração e envio desta comunicação.

(iii) Comunicação ao Cliente

Quando um incidente acionar o Plano de Continuidade de Negócios e afetar dados sensíveis, a Instituição deve comunicar de forma clara e tempestiva os clientes impactados.

A comunicação será realizada pelo e-mail institucional dpo@warren.com.br, além de disponibilizar canais exclusivos de atendimento para esclarecimentos adicionais.

O comunicado deve prezar pela transparência, trazendo informações objetivas sobre:

- Natureza do incidente;
- Medidas de contenção adotadas;
- Eventuais orientações de segurança ao cliente.

(iv) Iniciativas para Compartilhamento de Informações sobre os Incidentes Relevantes

A Instituição reconhece a importância da cooperação no enfrentamento de ameaças cibernéticas e participa ativamente do MISP Project (Malware Information Sharing Platform), utilizando o servidor disponibilizado pela ANBIMA em conjunto com o Cert.BR.

Esse servidor é composto por diversas instituições financeiras, o que nos permite compartilhar informações relevantes sobre incidentes e ameaças direcionadas especificamente para o setor financeiro. O MISP (Malware Information Sharing Platform) é uma solução abrangente que facilita o compartilhamento seguro e eficiente de indicadores de comprometimento (IOCs), informações sobre ameaças, técnicas de ataque e outros dados relevantes. Ele oferece recursos avançados de agregação, correlação e visualização de informações, permitindo que as instituições financeiras colaborem ativamente no combate a ameaças cibernéticas. Através do MISP, é possível compartilhar informações sobre incidentes de segurança cibernética de forma confidencial, preservando a privacidade e a anonimidade das instituições participantes. A plataforma oferece recursos de compartilhamento seletivos, garantindo que apenas as informações relevantes e necessárias sejam compartilhadas entre os membros do setor financeiro.

Além disso, o MISP fornece recursos avançados de análise e inteligência de ameaças, permitindo que as instituições financeiras identifiquem padrões, tendências e potenciais ameaças emergentes com base nas informações compartilhadas.

A participação no MISP reforça o compromisso da Instituição em fortalecer a resiliência do setor financeiro, contribuindo para a cooperação coletiva contra ameaças cibernéticas.

5. Documentos Vinculados

Esta Política é complementada por um conjunto documentos que devem ser observados de forma integrada.

São eles:

- Plano de Continudade de Negócios;
- Plano de Recuperação de Desastre; e
- Procedimento de Gestão de Incidentes

6. Vigência

Esta Política entra em vigor na data da sua publicação e deve ser revisada, no mínimo, anualmente, bem como quando ocorrerem alterações significativas nos processos definidos neste documento.