PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)	Vigência	Documento
	09/08/2012	PCN001
	Versão	Página
	06	1 / 14

Nome da Atividade	Macroprocesso	Processo	Subprocesso
PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)	SEGURANÇA CIBERNÉTICA	CONTINUIDADE DE NEGÓCIOS	GERIR RISCOS E DANOS

1. Sumário Executivo

Objetivos do Plano:
• Definir as regras aplicáveis com base na estrutura da C&M Software e
• Assegurar que todos conheçam o Plano de Continuidade de Negócio (PCN).

Processos Vitais:
a) Garantir o pleno funcionamento de nossos clientes perante o Sistema Financeiro Nacional, subentende-se: SPB, OBE, SPI
b) Garantir a execução, da parte sob a responsabilidade da C&M Software, dos processos críticos de nossos clientes – liquidações financeiras, abertura de contas, ofertas de crédito, etc, subentende-se Rocket e seus módulos

Site de Contingência: Equinix Data Center - SP2

Localização:	**Alameda Araguaia, 3641 - Tamboré, Barueri - SP, 06455-000**
Acesso via Portal:	**https://customerportal.equinix.com/**
Telefones:	**(11) 3524-4300** **0800.892.5065**
E-mail:	**support@equinix.com**

Responsáveis pela Continuidade do Negócio:

Staff	Nome	Telefones
Diretor de Operações	**André Ferreira**	**Celular: 11 99172.7766** **Celular: 11 97632.1796**
Gerência de Operações	**Leandro Souza**	**Celular: 11 97670.8082** **Celular: 11 96716-2967**

2. Introdução

O PLANO DE CONTINUIDADE DE NEGÓCIOS **PCN-001** complementa a POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA e assegurará à C&M Software a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos.

3. Objetivo

O Plano de Continuidade de Negócios (PCN) tem o objetivo de atender as normas e legislação vigentes que obrigam as instituições financeiras que utilizam os serviços de Provedores de Serviços de Tecnologia da Informação (PSTI) a implementar, em sua estrutura de gerenciamento de risco operacional, o Plano de Continuidade de Negócios (PCN).

O PCN deve ser acionado quando houver a inoperância total ou parcial do ambiente de produção da C&M Software motivado por alguma catástrofe no seu site principal ou em alguma situação, por ela, declarada.

4. Aplicação e Vigência

Este plano documentado aplica-se a todos Departamentos da C&M Software e vigorarão por prazo indeterminado.

5. Definição das Ações e Pessoas Envolvidas

Os processos críticos ao negócio da C&M Software foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio.

Para tanto, o PCN é definido como (PCN = PAC + PRD + PCO), a saber:

• **PAC = Programa de Administração da Crise** – É acionado após decretada a Crise, e é voltado para todo o processo. Mede os impactos e sua criticidade. Feito isso, define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes, durante e após a ocorrência. Tem seu término quando se volta à normalidade;

Pessoas Envolvidas, e ações:

Operadores

1) Havendo disponibilidade de acesso e infraestrutura, efetuar:
   - uma varredura na monitoria para auxiliar na identificação e extensão do problema.
   - executar as rotinas de teste básicos de conectividade e funcionalidade.

2) Uma vez confirmado o problema, manter a estrutura de atendimento a clientes dos canais telefone, e-mail, chat, WhatsApp.
3) Entrar em contato com fornecedores, se necessário.
4) Entrar em contato com o contingente da equipe de Operadores, se necessário, para auxiliar no atendimento aos clientes.
5) Acionar as respectivas equipes de Analistas de Suporte e Equipes de Produto.

Analistas de Suporte, Equipes de Produto e seus Coordenadores

1) Avaliar os sistemas e recursos afetados.
2) Avaliar os fornecedores.
3) Avaliar sequência de procedimentos.
4) Iniciar procedimentos de Contingência, se necessário.
5) Iniciar os procedimentos para reestabelecimento dos sistemas.

• **PRD = Plano de Recuperação de Desastres** – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN.

Pessoas Envolvidas, e ações:

Analistas de Suporte, Equipes de Produto e seus Coordenadores

1) (coordenadores) Definir procedimentos que serão necessários relativos a backup, consertos e manutenções.
2) (coordenadores) Definir fornecedores que deverão ser acionados para reparo de infraestrutura.
3) (analistas) Efetuar procedimentos de restauração de backup, consertos e manutenções.
4) (analistas) Acompanhar tarefas executadas por fornecedores.
5) (coordenadores) Efetuar o acompanhamento das tarefas e equipe durante o processo.
6) (coordenadores) Definir com segurança a finalização da ocorrência e procedimentos para o retorno dos sistemas a formação original.
7) (coordenadores) Elaboração de relatórios do incidente.
8) (diretoria) Eventual comunicação do evento aos clientes.
9) (coordenadores) Revisitar o evento, e todas as suas consequências, para verificar se o PCN está adequado para tal especificidade.

• **PCO = Plano de Continuidade Operacional** – São acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio;

Pessoas Envolvidas, e ações:

Coordenadores
1) Avaliar necessidades de melhorias.
2) Avaliar pontos pendentes de redundância.
3) Efetuar orçamentos.

Diretoria de Suporte
1) Aprovação de Orçamentos

Presidência
1) Aquisições

O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

• Análise de riscos de TI;
• Análise de Impacto nos Negócios (BIA);
• Estratégia de recuperação.

Desta forma será necessário simular situações de emergência, definir responsabilidades e escopo de atuação para cada colaborador na execução do PCN. A manutenção do PCN atualizado e o treinamento dos colaboradores são fatores crítico de sucesso.

6. Plano de Contingência

Deve ser utilizado quando as medidas de prevenção tiverem falhado (redundância de links, discos, fornecimento elétrico). Define as necessidades e ações mais imediatas.

6.1 Topologia

A C&M Software conta com duas unidades: a principal e a de redundância.
A unidade principal (Site Principal) situa-se à Alameda Rio Pardo 27, Barueri, São Paulo, onde a administração de seus produtos é executada em condições normais.

A unidade de redundância (Site Redundância) contém exatamente todos os mesmos recursos tecnológicos da Unidade Principal, podendo cada produto utilizar tanto a Unidade Principal como o Site de Redundância. Portanto, em situações de contingência, os funcionários designados devem se dirigir para esse endereço de forma que haja o mínimo impacto possível dentro das atividades da Plano de Continuidade de Negócio.

Site de Redundância: Equinix Data Center - SP2

Localização:	**Alameda Araguaia, 3641 - Tamboré, Barueri - SP, 06455-000**
Acesso via Portal:	**https://customerportal.equinix.com/**
Telefones:	**(11) 3524-4300** **0800.892.5065**
E-mail:	**support@equinix.com**

O Site Principal e Site Redundância possuem estruturas atualizadas com recursos para ativação total ou parcial dos serviços. Sendo em sua visão geral: servidores de enfileiramento, servidores web, servidores de banco de dados, e servidores de processamento.

Em função do site de redundância atender os processos críticos em caso de contingência, segue abaixo a designação do local que os colaboradores das áreas devem se dirigir nessas situações:

Área	Local de Contingência
Risco e Compliance	Home Office
Comercial	Home Office
Administrativo/Financeiro	Home Office
Marketing	Home Office
Modelos Preditivos	Home Office
TI	Depende da situação

6.2 Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no item 7 – Processos e Sistemas Críticos.

6.3 Monitoração de Comunicação de Eventos

Qualquer colaborador da C&M Software, ao constatar alguma anormalidade que paralise quaisquer processos apontados no item 7 deste Plano deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato a um dos Líderes de Contingência, a saber:

Staff	Nome	Telefone	E-mail
Diretor de Operações	André Ferreira	Celular: 11 9172.7766 Casa: 11 97632.1796	andre.ferreira@cmsw.com
Gerência de Operações	Leandro Souza	Celular: 11 97670.8082 Celular: 11 96716-2967	leandro.souza@cmsw.com

6.4 Declaração de Desastre/Contingência

Ao ocorrer quaisquer eventos que paralise algum processo essencial ao negócio, a Gerência de Operações avaliará a ocorrência e comunicará ao Diretor responsável pelo PCN. Com base nas informações recebidas e avaliação do grau de impacto versus horário crítico, compete ao Diretor declarar ou não a contingência.
Em caso da ausência do Diretor responsável pelo PCN assumirá interinamente o a Gerência de Operações. No **ANEXO 1** está descrito o Fluxo de Acionamento do PCN que resultará ou não na declaração da contingência.

6.5 Suporte e Atendimento ao Cliente

Visando entregar qualidade, a C&M Software adota como uma das suas principais missões fornecer um atendimento eficaz ao cliente e resolver seus eventuais problemas. Cada situação citada é classificada por um código, de acordo com os dados abaixo:

Código 1: Alto Impacto

❑ Requer imediata atenção e encaminhamento para outros níveis de suporte.
❑ O problema não está sendo contornado e está afetando a produção da companhia.

Código 2: Médio Impacto

❑ Algumas funcionalidades estão com dificuldade de execução.
❑ O produto opera, mas com algumas restrições.
❑ A situação ocorre mais de 2 vezes por semana.

Código 3: Baixo Impacto

❑ A maioria das funções continua funcionando normalmente, mas alguma anomalia ocorre com o produto.
❑ A situação ocorre menos de uma vez por semana.

Código 4: Sem Impacto

❑ Dúvidas com relação à implantação e utilização do produto.

Código	Horário Comercial	Plantão
Código 1	Na Mesma Ligação	100% em 1 Hora
Código 2	95% em 2 Horas	Dia Seguinte
Código 3	95% em 4 Horas	Dia Seguinte
Código 4	95% em 8 Horas	Dia Seguinte

Help Desk [24 x 7]: 55.11.3365.2666
E-mail: suporte@cmsw.com

7. Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, definido pela fórmula (MTD = RTO + WRT).

Definição:
- MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de negócio em particular. Diferentes funções de negócio terão diferentes MTD's.

- RTO (Recovery Time Objective) = Tempo disponível para recuperar sistemas e recursos de uma ruptura.

- WRT (Work Recovery Time) = Tempo que leva para copiar e rodar uma vez os sistemas (hardware, software e configuração) a serem restaurados para as funções de negócios críticas.

7.1 Processos com MTD de até 30 minutos

Área	Processos	Sistemas
Tecnologia da Informação	Liquidações financeiras, abertura de contas, ofertas de crédito	Todos

7.2 Processos com MTD IMEDIATO das 06:00h até 18:30h

Área	Processos	Sistemas
Tecnologia da Informação	Garantir o pleno funcionamento de nossos clientes perante o Sistema Financeiro Nacional	SPB, OBE

7.3 Processos com MTD IMEDIATO 24x7

Área	Processos	Sistemas
Tecnologia da Informação	Garantir o pleno funcionamento de nossos clientes perante o Sistema Financeiro Nacional	SPI, Domínio - SPB02

8. Abrangências

8.1 Ameaças Relacionadas

No entendimento dos gestores das áreas avaliadas as ameaças com grau de vulnerabilidade significante estão divididas em:

a. Humanas
Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.

b. Tecnológicas
Falha em Aplicativo (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.

c. Infraestrutura
Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.

d. Naturais
Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio.

e. Físicas
Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis aos negócios da C&M Software, acarretando perda de confiança de colaboradores e clientes nos processos de negócios. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

• Interrupção de prestação de serviços a clientes;
• Multas e sanções;
• Perda da capacidade de gestão e controle;
• Comprometimento da imagem da organização;
• Exposição negativa na mídia e perda de vantagem competitiva.

9. Ações e Procedimentos

** Todos os procedimentos devem ser registrados e se possível fotografados. **

Qualquer colaborador deverá estar apto a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao diretor de Operações.

9.1 Impossibilidade de Acesso ao Prédio

Dentre as ameaças que impossibilitam o acesso ao prédio destacamos:

• Princípio de Incêndio;
• Ameaça de Bomba;
• Bloqueios;
• Manifestações

9.1.1 Ações de 05 a 10 minutos após a evidência

Responsável: Diretor de Operações

Procedimentos:
A Área Administrativa entrará em contato com os seguintes órgãos públicos:

• Bombeiros: **193** (Incêndio e Ameaça de Bomba);
• Defesa Civil: **199** (Ameaça de Bomba, Greves, Bloqueios e Inundações);
• Polícia Civil: **147** (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

9.1.2 Ações em até 20 minutos após a conclusão da etapa anterior

• Entrar em contato com o responsável pelo site backup, conforme indicado no Sumário Executivo, para avisá-lo sobre a ocupação dos integrantes das áreas contingenciadas e disponibilizar local, notebook e impressora, assim como acesso à Internet, bem como avisar os componentes que atuarão em regime Home Office.

• Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço do site redundância, ou as residências para atuação no regime Home Office, conforme relação indicada abaixo:

Área Contingenciada	Nome	Contato	E-mail
Diretor de Operações	André Ferreira	11 99172.7766	andre.ferreira@cmsw.com
Comercial	Kamal Zogheib	11 97684-6892	Kamal.zogheib@cmsw.com
Administrativo / Financeiro	Selma Oliveira	11 98522-8241	selma.oliveira@cmsw.com
Risco & Compliance	Rui Saraiva	11 98444-3242	rui.saraiva@cmsw.com
Suporte e Operação	Leandro Souza	11 97670.8082 11 96716-2967	leandro.souza@cmsw.com

Disponibilizar alertas no site da C&M Software indicando o status de contingência, telefones dos colaboradores e telefone fixo do site backup para atendimento.

9.2 Falha na Infraestrutura e Tecnologia

Para não haver interrupções nas atividades o ambiente de TI no site principal da sede a Unidade de Redundância será o site de contingência da sede.

A comunicação entre as unidades de negócio é feita por links redundantes. A seguir destacamos a infraestrutura de TI de cada unidade de negócio.

• Servidores
• Telecom
• Energia Elétrica

Na falta de energia elétrica, além das baterias próprias dos Notebooks, são ativados automaticamente os nobreaks localizados no site principal no CPD com autonomia de 2 horas.

As áreas abastecidas pelos Nobreaks são as mesmas mapeadas com processos críticos pelo BIA.

- Tecnologia da Informação
- Administrativo/Financeiro
- Gestão de Riscos e Compliance

9.3 Acionamento da Contingência externa

Manter contato com o gestor da empresa contratada para prestação de serviços de redundância / backup e contingência e avisar do início do processo de contingência. As equipes irão para o lugar destinado a cada uma delas.

Manter contato com a empresa ONE PBX – Pedro Csordas – Tel. (11) 98912-8712 (Manutenção do PABX) e solicitar o encaminhamento de todas as ligações para os ramais do escritório do Site de Contingência, se for o caso.

10. Procedimentos de retorno à normalidade – Site Principal

Cabe ao diretor de Operações encerrar o PCN e comunicar aos Gestores envolvidos no processo.
Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores da C&M Software por meio de seus gestores para que retornem aos seus postos de trabalho no dia seguinte.
Solicitar à área de TI que retire o comunicado publicado no site da C&M Software sobre a situação de contingência.

11. Administração do Plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias.

O processo de Continuidade de Negócios é de responsabilidade do Comitê de Segurança de TI, que determina o ciclo e as etapas que deverão ser executadas para

que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios da C&M Software.
Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado, os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

11.1 Divulgação e Treinamento

Um dos fatores de primordiais para o funcionamento deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento.
Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a equipe da C&M Software definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios.
Estas sessões serão organizadas pela área de Segurança da Informação e Compliance em conjunto com a área de Administrativa/Financeira com o objetivo de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.
Para que este conhecimento seja preservado, os colaboradores admitidos e os transferidos para funções de negócios críticas, principalmente aqueles que pertencem à equipe de contingência, deverão ser instruídos das suas respectivas responsabilidades no plano.
O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

11.2 Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação.
A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, que dever ser arquivado por um período mínimo de 5 (cinco) anos.
Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da C&M Software e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

12. Revisões

Esta política de PCN é revisada **trimestralmente** pelo **Comitê de Segurança da TI**.

13. Gestão do PCN

A política de PCN é aprovada pelo Comitê de Segurança de TI, em conjunto com a Diretoria da C&M SOFTWARE LTDA.

A presente política de PCN foi aprovada no dia 09/08/2012

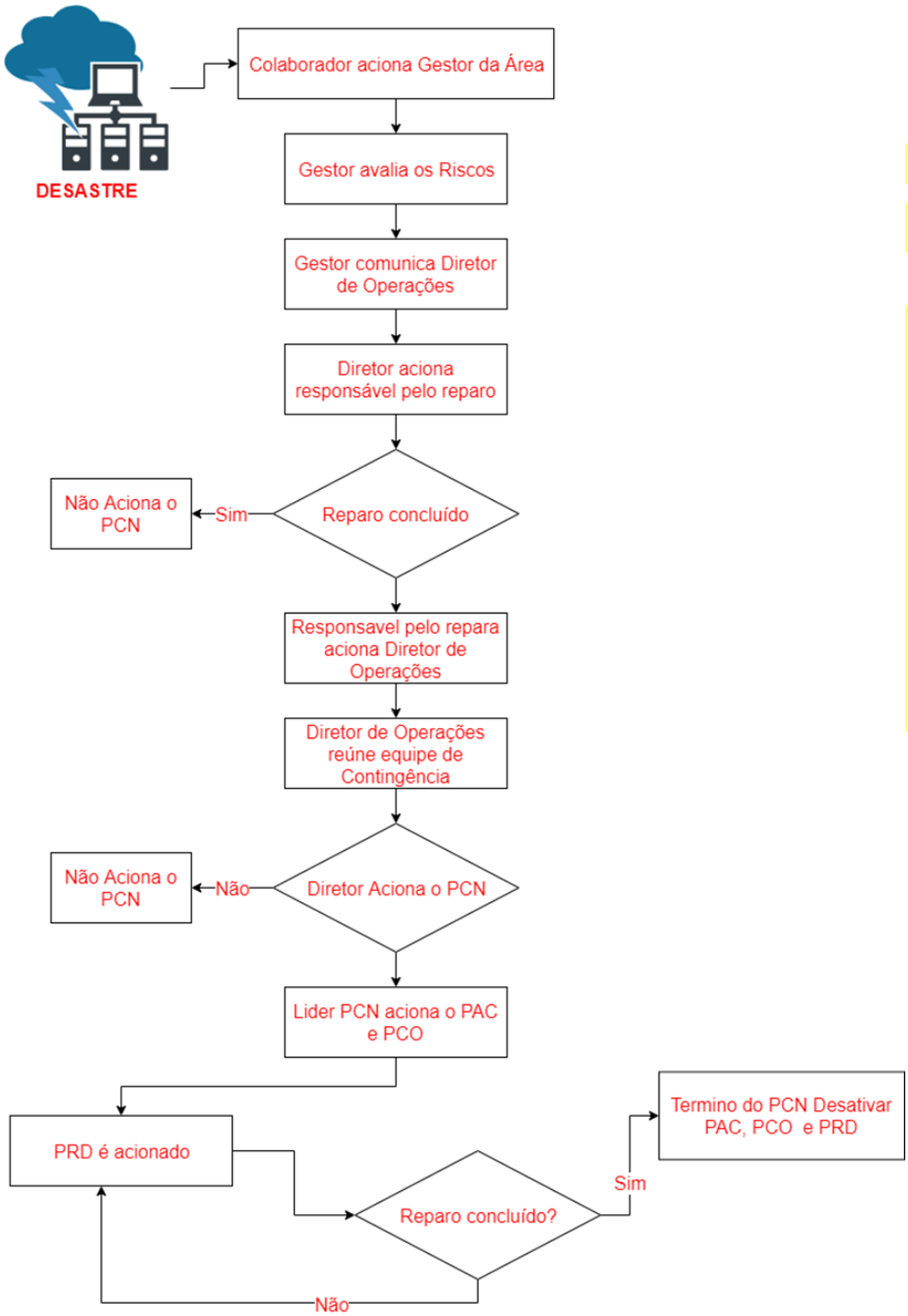
Histórico das Revisões

Versão	Motivo	Data Revisão	Atualizado por	Divulgação
6	Revisão Geral	06/11/19	Márcio Borges André Ferreira	06/11/2019

PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)	Vigência	Documento
	09/08/2012	PCN001
	Versão	Página
	06	14 / 14

Nome da Atividade	Macroprocesso	Processo	Subprocesso
PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)	SEGURANÇA CIBERNÉTICA	CONTINUIDADE DE NEGÓCIOS	GERIR RISCOS E DANOS

ANEXO 1



Elaborado por:	Revisado por:	Aprovado por:
Márcio Borges – Segurança da Informação	Leandro Souza – Suporte e Operação	André Ferreira – Diretor de Operações