Plano de Contingência e Continuidade dos Negócios

EMPRESA: GRUPO ECOAGRO

ÁREA RESPONSÁVEL: TECNOLOGIA DA INFORMAÇÃO

CÓDIGO: PO-ECO-06

VERSÃO: 04

DATA PUBLICAÇÃO: 26/11/2025

VIGÊNCIA: 26/11/2027

CLASSIFICAÇÃO DA INFORMAÇÃO: PÚBLICA

Plano de Contingência e Continuidade dos Negócios

ÍNDICE

Plano de Contingência e Continuidade dos Negócios

1. Introdução

O Plano de Continuidade dos Negócios (“PCN”) é uma ação preventiva, que visa prover a empresa de procedimentos, controles, responsabilidades e regras, permitindo a continuidade das operações de suas áreas de negócio após eventuais ocorrências que impossibilitem a utilização parcial ou total da plataforma operacional do GRUPO ECOAGRO.

O PCN prevê ações que durem até o retorno à situação normal de funcionamento do Grupo ECOAGRO dentro do contexto de seu negócio e para isso, uma análise de riscos potenciais, estratégias e planos de ação foram elaborados com o intuito de garantir que os serviços essenciais do Grupo ECOAGRO sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

2. Objetivo

O presente PCN tem como objetivo estabelecer diretrizes para a implementação de plano destinado a assegurar a continuidade operacional do Grupo Ecoagro, nos casos de situações emergenciais que possam afetar parcial ou totalmente as suas atividades.

3. Público-Alvo

O presente documento deve ser observado por todos aqueles que possuam cargo, função, relação societária, empregatícia, comercial, profissional, contratual ou de confiança com o GRUPO ECOAGRO, inclusive a Diretoria ou Alta Administração do GRUPO ECOAGRO. Na atribuição de suas atividades, devem observar os melhores esforços a partir das orientações previstas no presente documento, considerando-se as necessidades específicas e os aspectos legais e regulamentares aos quais estão sujeitas as atividades para gestão de recursos.

4. Planos

O Plano é integrado por um plano de backup e pelos planos de emergência e recuperação. Estes planos deverão ser acionados sempre que houver um incidente e ficarão ativos até a recuperação total da empresa.
O PCN também visa garantir a segurança e proteção dos Sistemas de Informação do Grupo ECOAGRO, assegurando a continuidade de todo o processo tecnológico vital aos negócios.
O detalhamento abaixo apresenta brevemente o objetivo e escopo de cada plano para o enquadramento de cada cenário de crise:

O PCN é definido como (PCN= PAC + PCO + PRD), a saber:

Plano de Contingência e Continuidade dos Negócios

PAC: É acionado após decretada a crise para proporcionar condições de continuidade do negócio como um todo.

PCO: Direcionar ações iniciais com o objetivo de dar continuidade às rotinas operacionais essenciais.

PRD: Designar meios para recuperação/restauração de componentes que suportam o PCN, auxiliando no restabelecimento da continuidade operacional.

Tipo de Plano	Plano de Contingência (PC)	Plano de Administração de Crises (PAC)	Plano de Recuperação de Desastres (PRD)
OBJETIVO	Direcionar ações iniciais com o objetivo de dar continuidade às rotinas operacionais essenciais.	É acionado após decretada a crise para proporcionar condições de continuidade do negócio como um todo.	Designar meios para recuperação/restauração de componentes que suportam o PC, auxiliando no restabelecimento da continuidade operacional.
ESCOPO	Ocorrências de maior probabilidade e pouca intensidade desastrosa, construído a partir de cenários prováveis/previamente definidos e de rápida resolução.	Ocorrências de menor probabilidade com possível prejuízo nas estruturas de Infraestrutura, TI ou ambiente, construído a partir de cenários inesperados.	Acidentes inesperados, considerando limitações de acesso às estruturas, construído a partir do cenário de desastre.
EXEMPLO DE CENÁRIOS	Descontinuidade no fornecimento de energia elétrica, água, telefonia e Internet.	Invasão de vírus destruidores de dados, perda de disco rígido/ servidor, falha no ar-condicionado/ de energia	Avaria grave nas estruturas físicas/incêndio.

		de maior proporção, ameaça de ameaça biológica (pandemias ou endemias).	

5. Responsabilidades

As seguintes atribuições/responsabilidades são designadas no que tange este PCN:

Diretoria: será de responsabilidade da Diretoria gerenciar o PCN, manter e proporcionar condições para a operacionalização e funcionalidade do PCN, conforme a natureza do acidente, além de será responsável também pela aprovação deste Manual e seus procedimentos sempre que houver alterações.

TI: será responsável pelo teste e operacionalização do PCN no que tange à Tecnologia e Segurança da Informação e informar a área de Compliance e Controles Internos sempre que houver alterações sistêmicas.

Administrativo/RH: será responsável pelo teste e operacionalização do PCN no que tange à notificação de incidentes, pessoas, relacionamento com administração predial e demais prestadores de serviço para funcionalidade do PCN.

Compliance e Controles Internos: área responsável por acompanhar execução dos testes periódicos e prover suporte para melhoria contínua.

Comitê de Gerenciamento de Crise: responsável por coordenar os esforços para levantamento de informações relevantes, coordenação da comunicação oficial do Grupo ECOAGRO e demais atividades para gerenciamento de crise. Será constituído quando a situação de recuperação tenha um prazo longo ou demandar decisões diferentes as já dispostas neste plano, sendo convocado pelo Diretor de Compliance e Controles Internos. Este comitê será composto pelo Diretor de Compliance e Controles Internos e demais sócios diretores, com suporte das áreas de Tecnologia, Recursos Humanos, Compliance e Controles Internos e demais áreas de apoio.

Plano de Contingência e Continuidade dos Negócios

6. Recursos

Os recursos disponíveis encontram-se sumarizados na tabela abaixo:

RECURSOS	ÁREA RESPONSAVEL	Detalhamento do Recurso
Energia elétrica	Administrativo	Energia proveniente da fornecedora local e dois geradores, um para as áreas privativas e outro para as áreas compartilhadas. Autonomia de 8 horas para as áreas privadas do condomínio.
Água	Administrativo	Caixa d'água com capacidade de fornecimento para toda a empresa, por período indeterminado. Água com captação por meio de poço, com utilização de bomba hidráulica.
Internet	Tecnologia da Informação (TI)	Link de fibra ótica, (operadora VIVO) Link de fibra ótica (operadora Neotelecom) Link de fibra ótica (operadora Mundivox)
Telefonia	Tecnologia da Informação (TI)	PABX virtual e celulares fornecidos pela empresa.
Servidores arquivos	Tecnologia da Informação (TI)	4 servidores, sendo 1 de arquivo, 1 de impressão, 1 de autenticação de usuário e 1 redundância de autenticação
Estações de trabalho	Tecnologia da Informação (TI)	Notebooks Desktops
Segurança de Rede	Tecnologia da Informação (TI)	*Firewall* com redundâncias, *Endpoit Protection* (Antivirus, *firewall*, criptografia e agente de e-mail), Sistema de inventário de hardware e software.
E-mail	Tecnologia da Informação (TI)	Serviço de e-mail em nuvem.
Ambiente cloud	Tecnologia da Informação (TI)	Ambiente da AWS com 20 servidores VPN para conexão com a rede interna
Espaço físico	Administrativo	Escritório localizado na avenida Pedroso de Morais, n°1553 nos conjuntos 31,32,33,34, 81 e 84.

Sistemas	Tecnologia da Informação (TI)	Consultar Inventário de Sistemas
Site Institucional	Marketing	Site hospedado na AWS
Link de conexão com B3	Tecnologia da Informação (TI)	Link de dados com RTM

7. Estratégias

Considerando-se os vários cenários que possam ocorrer durante o ciclo operacional do Grupo Ecoagro, as orientações do quadro abaixo servem como diretriz para as tomadas de ações necessárias para o restabelecimento dos acessos e serviços:

CENÁRIO	PCO (Plano de Continuidade Operacional)	PAC (Plano de Administração da Crise	PRD (Plano de Recuperação de Desastre)
Ataque Cibernético	Restaurar em um diretório de nuvem os arquivos essenciais para a continuar as operações conforme as permissões de cada usuário.	Localizar a origem do ataque e tomar as medidas cabíveis para cessar o incidente.	Subir novamente o ambiente, restaurando todos os dados do backup e autorizar as permissões conforme definido antes do ataque.
Falta de Energia Elétrica	Geradores são acionados para substituir a rede elétrica de distribuição.	Caso não haja o restabelecimento colocar colaboradores em acesso remoto.	Acionar o condomínio para solicitar providências e prazos de restabelecimento.

Plano de Contingência e Continuidade dos Negócios

Falta de Água	Contatar condomínio para a contratação de caminhão pipa e utilização da água da caixa d'água até a normalização.	Caso não haja o restabelecimento colocar colaboradores em acesso remoto.	Acionar o condomínio para solicitar providências e prazos de restabelecimento.
Falta de Conexão à Internet	Firewall monitora sinal de Internet caso haja falha no link principal, distribui o tráfego entre os demais.	Caso não haja o restabelecimento colocar colaboradores em acesso remoto.	Contatar operadora para restabelecimento do link ou substituição da operadora.
Falha na telefonia	Direcionamento automático para os celulares corporativos, via aplicativo do PABX virtual.	Utilização dos celulares até normalização da situação.	Entrar em contato com a empresa que administra a telefonia fixa para restabelecimento.
Falha no ar-condicionado das áreas privativas	Abertura de Janelas	Os membros responsáveis pelo Comitê de Gerenciamento de Crise deverão avaliar as proporções e impactos e caso identifique uma situação crítica, os colaboradores serão orientados para Trabalho Remoto.	Acionar a equipe de manutenção do condomínio para corrigir falhas.
Falha no ar-condicionado do servidor	Providenciar ventilação mecânica para a sala, se necessário alugar máquina de ar portátil.	Acompanhar a temperatura da sala constantemente.	Enviar equipamento para conserto e/ou substituição permanentemente.

Falhas no servidor	Backup será restaurado em área restrita nos servidores que estiverem ativos ou nas estações, ou em local na nuvem.	Manter arquivos disponíveis nos servidores até a nova área definitiva.	Subir novamente o ambiente, restaurando todos os dados do backup e autorizar as permissões conforme definido antes do ataque. Orientar os colaboradores para continuidade das atividades por meio de Trabalho Remoto.
Falha em estações de trabalho	Colocar equipamento reserva para o usuário.	Manter equipamento reserva com os dados necessários para o usurário poder seguir com suas atividades.	Enviar equipamento para conserto e/ou substituição permanente.
Incêndio	Enviar colaboradores para o trabalho remoto provendo equipamentos reservas caso necessário.	Comunicação imediata ao Comitê de Gerenciamento de Crise e à Brigada de Incêndio para combate ao foco de incêndio por meio de extintores e reservatório de água. Acionamento do Corpo de Bombeiros através do condomínio caso o incêndio seja de grandes proporções Será acionado o Comitê de Gerenciamento de Crise para avaliar as proporções do dano e as medidas necessárias para o acesso remoto.	Realizar as devidas reformas no local ou alugar tempestivamente um novo local.
Greve de transporte público.	Carro de aplicativos ou trabalho remoto.	Os colaboradores utilizam transportes particulares ou	Aguardar a normalização do

		carro por aplicativo ou realizam trabalhos remoto.	transporte público. Os colaboradores utilizam transportes particulares ou carro por aplicativo.
Manifestações que impeçam acesso às dependências	Os responsáveis deverão se reunir para avaliação da situação orientando o trabalho remoto.	Durante o período de manifestação será mantido o trabalho remoto, fornecendo equipamentos a quem não consiga pegar o equipamento que ficou na empresa.	Aguardar fim da manifestação.
Inundações	Os responsáveis deverão se reunir para avaliação da situação orientando o trabalho remoto.	Durante o período será mantido o trabalho remoto fornecendo equipamentos a quem não consiga pegar o equipamento que ficou na empresa.	Aguardar fim da inundação.
Risco de Ameaça Biológica (Quarentena)	Colaboradores devem ficar em trabalho remoto.	Acionar o Comitê de Gestão de Crise Restringir acesso ao escritório Todos trabalham em regime remoto Viagens suspensas Fornece suporte para execução das atividades críticas Providenciar apoio aos colaboradores Acompanhar diretrizes dos órgãos responsáveis. Elaborar plano de retomada de acesso ao escritório & adequação às diretrizes emitidas pelos órgãos responsáveis. Fornecer transporte não-coletivo aos colaboradores	Aguardar fim da ameaça com a liberação das autoridades competentes.

		que precisarem acessar o escritório. Elaboração da Política de Conduta no escritório durante o risco de ameaça. O Comitê de Gestão de Crise deve coordenar as atividades para retomada da normalidade, conforme plano estabelecido.	
Falha Link RTM	Realizar operação pelo site da B3.	Realizar operação pelo site da B3.	Solicitar restabelecimento do link para RTM.
Sala de Contingência na RTM	Dispõe de uma sala de contingência estruturada para garantir a continuidade das operações críticas em caso de indisponibilidade do ambiente principal. O espaço conta com infraestrutura de rede, equipamentos e acessos necessários para que as atividades essenciais sejam retomadas com o mínimo de interrupção.	Em situações de crise, a sala de contingência serve como ponto centralizado de acesso ao Cetip para equipe de operações. O ambiente garante comunicação e acesso às informações necessárias para que as decisões sejam tomadas de forma ágil e organizada.	A sala de contingência é ativada como parte do processo de recuperação em cenários de desastre, permitindo que as equipes de tecnologia e operações trabalhem na restauração dos sistemas B3 Cetip a partir de um ambiente seguro e funcional, reduzindo o tempo de indisponibilidade.

8. Declaração de Incidente/Contingência

Ao ocorrer eventos que paralisem processo(s) essencial(is) ao negócio, um dos responsáveis das áreas operacionais deverá avaliar a ocorrência/incidente e comunicar a área de Administrativa ou TI a depender do caso. Este, por sua vez, receberá os alertas, determinará quais as ações a serem executadas com base neste Plano e, quando apropriado, acionará o Comitê de Gerenciamento de Crise.
A notificação de incidentes poderá ser feita por qualquer integrante das equipes.

Plano de Contingência e Continuidade dos Negócios

9. Metodologia de Comunicação

9.1 Comunicar aos colaboradores

Ao ocorrer eventos que paralisem processo(s) essencial(is) ao negócio, o responsável de cada área deverá comunicar por meio de contato telefônico ou por e-mail para este fim, para que todos os envolvidos se mantenham informado do incidente e da inatividade dos serviços.

9.2 Comunicar aos terceiros

O Grupo ECOAGRO junto aos responsáveis de cada área responsável pelo incidente deverá fornecer informações pertinente aos terceiros como: Clientes, parceiros, cidadãos e outros órgãos caso necessário.

9.3 Comunicar as autoridades

O Grupo ECOAGRO será responsável por comunicar através do grupo de WhatsApp Arvores de Chamados administrado pelo RH, Compliance e Controles Internos, Tecnologia da Informação e Diretoria os incidentes ocorridos, principalmente se envolver risco às pessoas, informando a localização, natureza e impacto do desastre

9.4 Comunicar retorno das operações

O Grupo ECOAGRO deverá comunicar todas as partes acima o retorno das operações à normalidade através do grupo de WhatsApp Arvores de Chamados administrado pelo RH, Compliance e Controles Internos, Tecnologia da Informação e Diretoria.

10. Ponto de Encontro

O Grupo ECOAGRO possui uma estrutura localizada na unidade *Self Storage GoodStorage*, Av. Pedroso de Morais, 613 - Pinheiros, São Paulo - SP, 05419-000, onde estão armazenados equipamentos para substituições emergenciais, conta com uma estrutura mínima para operações de emergência, com acesso à internet. Conforme contrato de locação do box, ficam disponibilizadas salas de reuniões no local.

11. Trabalho Remoto

O Grupo ECOAGRO possui notebooks próprios, devidamente autorizados, com acesso à Internet e com acesso aos dados por VPN (rede privada virtual). Segurança individual, por firewall e antivírus de end point com regras e controles centralizados. Todas as estações são monitoradas por software de inventario de hardware e software.

O Grupo também fornece celular com acesso ao ramal interno e internet rápida que possibilita conexão com as estações em qualquer lugar com cobertura móvel.

Na impossibilidade de se utilizar o espaço físico do escritório, o Grupo ECOAGRO deverá continuar suas atividades no formato Trabalho Remoto que se dará por meio de acesso remoto e celulares corporativos, disponibilizados para todos os colaboradores.

Os arquivos estão os armazenados em backup em nuvem e serão disponibilizados a todos os colaboradores através de unidades compartilhadas restritas pelas permissões concedidas a cada usuário e/ou departamento. A comunicação do início e/ou término do trabalho em Trabalho Remoto será feita através da arvore de chamada ou outro mecanismo definido pelo Comitê de Gerenciamento de Crise. Os funcionários em Trabalho Remoto devem conectar a internet e a VPN para se manterem atualizados com as normas de segurança, devem se manter atentos aos comunicados enviados pela arvore de chamada, e-mails e notificações nos celulares corporativos. Sempre que solicitado devem responder as solicitações comprovando que estão ativos e cientes. Qualquer indisponibilidade de recurso, devem comunicar ao seu superior imediato e as áreas de suporte.

12. Estrutura de Suporte

Em caso de necessidade de utilização da estrutura de contingência, as pessoas responsáveis pelas funções críticas da empresa terão acesso às informações independentemente do acesso físico ao escritório, por meio de acesso remoto. Suporte técnico será realizado por plataforma de acesso remoto com acesso apenas com senha e consentimento do usuário.

13. Mapeamento de Atividades Críticas

Formulário de Mapeamento das Atividades Críticas, a matriz tem por objetivo a identificação de quais

ações devem ser tomadas para minimizar os impactos detectados em casos de interrupções nos negócios para que o Grupo ECOAGRO possa mensurar o impacto do tempo de inatividade, levando em consideração a priorização sobre as atividades "*Core Business"* da organização.

14. Programa de Testes

Os planos de ação elaborados, assim como as metodologias previstas no presente documento para remediar eventuais contingências e garantir a continuidade das atividades do Grupo ECOAGRO, são testados periodicamente em prazos não maiores que a cada 12 (doze) meses.

Os testes compreendem simulações de contingências para verificação da tempestividade e eficácia dos procedimentos desta política interna e envolverão a equipe responsável, conforme item 06 acima, e os profissionais da Área de TI, todos sob a coordenação do Diretor de Compliance, Riscos e Controles, conforme tabela abaixo:

Tipo	Teste	Periodicidade
Mesa	Revisão do PCN	Bianual
Atividades críticas	Link	Trimestral
	Restauração de *backup*	Trimestral
Simulação	Acesso remoto	Semestral
	Campanha de *Phishing*	Dois testes mensais
	Ataque Cibernético - *Pentest*	Anual

15. Revisão do PCN

A revisão é iniciada pelo responsável de Compliance e Controles Internos em conjunto com a área de TI e Administrativo/RH, que aprovará o documento juntamente ao Diretor de Tecnologia da Informação e Diretor de Compliance e Controles Internos.

A revisão será devidamente anotada na tabela de controle ao final do documento para fins de evidência.

O documento poderá ser modificado em períodos menores que um biênio, caso haja mudança significativa na plataforma operacional.

A ECOAGRO realiza anualmente a sua atualização de contatos e informações para certificar-se de que os colaboradores poderão ser contatados em casos de emergências ou acionamento do PCN.

O processo é iniciado pelo responsável pela área de RH que envia comunicado interno para todos os colaboradores para atualização dos dados existentes na base corporativa.

16. Atividades Críticas

16.1. Link

Trimestralmente, o responsável por TI fará o teste de link. Este teste consiste em avaliar a performance dos links verificando se estão ativos e entregando os índices estabelecidos em contrato.

16.2. Restauração de Backup

Trimestralmente o responsável por TI restauração de arquivos fará a baixa dos backups para verificação da integridade dos dados, que são diariamente copiados, de maneira automática. Estes arquivos serão baixados por amostragem.

17. Simulação

17.1. Acesso Remoto Completo

O Grupo ECOAGRO realiza anualmente simulações, que consistem em testes de verificação de acesso remoto dos seus colaboradores, este teste consiste na realização das atividades do total de colaboradores em formato Trabalho Remoto (90% dos colaboradores na ocasião do teste*)* e visa saber se a infraestrutura está realmente preparada para atender a demanda em casos críticos onde todos devem ficar remoto. Neste teste, todos os colaboradores devem executar suas tarefas remotamente de sua residência ou local apropriado. Durante o teste o grupo de controle respondera um formulário onde indicará se conseguiu acesso aos programas, arquivos e demais recursos necessários para a execução de suas tarefas diárias, incluindo telefonia. O resultado será enviado ao departamento de controles internos que tabulará o resultado.

17.2. Campanha de *Phishing*

O Grupo ECOAGRO realiza, mensalmente, duas simulações de ataques de *phishing* com o objetivo de avaliar o nível de conscientização e a capacidade de resposta dos colaboradores frente a ameaças cibernéticas. As simulações são conduzidas por meio da plataforma *KnowBe4*, através do disparo de campanhas controladas que replicam cenários reais de *phishing*, permitindo mensurar o grau de percepção dos usuários e identificar vulnerabilidades comportamentais que possam representar riscos à segurança da informação do Grupo.

17.3. Ataque Cibernético – Pentest

O Grupo ECOAGRO realiza, anualmente, uma simulação que permite identificar lacunas nos controles de segurança, validar os procedimentos de resposta a incidentes e subsidiar a atualização dos planos de continuidade com base em evidências práticas. As simulações abrangerão os ambientes ativos como, infraestrutura de rede, sistemas críticos, e-mail corporativo, acesso não autorizado, vazamento de dados etc. Ao final do *Pentest*, espera-se obter, mapa de vulnerabilidades com classificação por criticidade e probabilidade de exploração, avaliação da maturidade dos controles de segurança existentes, plano de remediação com ações corretivas priorizadas. Após a conclusão da simulação entrega do relatório técnico completo com achados, evidências e recomendações, e se necessário atualização do PCN.

18. Revisões

VERSÃO	ALTERAÇÃO	DATA
1	Criação do documento para atendimento às exigências regulatórias.	04/02/2019
2	Criado Conselho de Crise, revisado procedimentos de Backup, revisado método de teste de Links.	23/04/2021
3	Atualização e melhoria dos procedimentos	08/11/2021
4	Atualização periódica	26/11/2025

19. Responsáveis

Etapa	Responsável	Cargo
Elaboração	Pâmela Mendes	Analista de Governança de TI
Revisão	César Alves	Head de Tecnologia da Informação
	Rodrigo Hirae	Head de Compliance e Controles Internos
Aprovação	Leandro Mattia	Diretor de Compliance e Controles Internos
	Marcello Albuquerque	Diretor de Tecnologia e Inovação