POLÍTICA DE GESTÃO DE CONTINUIDADE DO NEGÓCIO

POLI-0004-01

MANTENHA APENAS UM: CONFIDENCIAL | **RESTRITO** | USO INTERNO | PÚBLICO

Obs. Este documento contou com a contribuição da Innocenti Advogados (consultora externa)

Controle de Versões

Data	Versão	Comentários	Autor
01.06.2021	1.0	Versão Inicial	Mariana M. Carregaro
13.01.2024	2.0	Revisão	Mariana M. Carregaro
13.01.2025	3.0	Revisão	Mariana M. Carregaro

Identificação e Classificação

Código do Documento	Tipo	Classificação
POLI-0004-01	Política	Restrito

Equipe e Responsáveis Envolvidos

Profissionais Envolvidos
Mariana M. Carregaro – Consultora Externa (Innocenti Advogados)
Lidiane P. dos Reis Barros – Encarregada

Documentos de Apoio ou Relacionados

Documentos de Apoio
Política de Segurança da Informação (T.I.)
Política de Incidente de Segurança (T.I.)
Política de Gestão de Risco (T.I.)
Política de Backup e Restauração (T.I.)
Política de Notificação de Violação (T.I.)
Evidência e Controle das Vulnerabilidades Cibernéticas

Aprovação da Diretoria Responsável

Diretor Responsável	Ratificação	Data
Alexandre Gonçalves Duarte	APROVADO	13.01.2025

Introdução

Uma vez que falhas nos serviços de qualquer departamento podem impactar diretamente a continuidade da prestação dos serviços da **Epeople**, almeja-se com este plano prover medidas de proteção rápidas e eficazes para os processos críticos relacionados às atividades essenciais em casos de incidentes graves ou desastres. O plano de continuidade atuará como resposta aos resultados da Análise de Impacto nos Negócios e Análise de Riscos.

Escopo

O Plano de Continuidade (PC) abrange as estratégias necessárias à continuidade dos serviços essenciais: contingência, continuidade e recuperação. Está voltado a conceder continuidade aos processos definidos como críticos para a **Epeople** e serviços essenciais prestados aos seus clientes.

Serviços Essenciais

Legenda:

- ✓ **TR**: Tempo para restauração do serviço.
- ✓ **GAP**: Ponto na linha do tempo que o serviço será recuperado.
- ✓ **SDI**: SLA de restauração de desastre e incidente contratado junto ao fornecedor de Data Center.
- ✓ **CCD**: Conforme Contrato de Serviço de Data Center.
- ✓ **UPD**: Up to Date, sem defasagem à data atual.
- ✓ **D-1**: Dia anterior à data atual.
- ✓ **Criticidade**: Importância do serviço ao negócio da **Epeople** (Alta / Média / Baixa / Indefinida).
- ✓ **Impacto**: Grau do efeito no serviço afetado (Alto / Médio / Baixo / Indefinido).

Riscos

Cenário de desastres que apresentam riscos à continuidade de negócio e disparam a execução deste plano:

Eventos de Desastre	Possíveis Causas
1 – Interrupção de energia	Causado por fator externo (manutenção) ou fator interno (curto-circuito, incêndio e infiltrações).
2 – Falha na climatização de salas essenciais	Superaquecimento de equipamentos e ativos devido a falha na climatização.
3 – Indisponibilidade de rede / circuitos	Rompimento de cabos de interconexão decorrente da execução de obras públicas, desastres ou acidentes.
4 – Falha humana	Dolo, culpa, imperícia ou imprudência ao manusear equipamentos ou informações.
5 – Ataques internos	Ataques aos ativos de informações e ao data center.
6 - Incêndio	Incêndio que comprometa a estrutura de T.I e documentos físicos (arquivos e armários).
7 – Desastres naturais	Terremotos, tempestades, alagamentos, raios etc.
8 – Falha de hardware	Falha que necessite reposição de peça ou reparo.
9 – Ataque cibernético	Ataque virtual que comprometa o desempenho, os dados, o acesso, a edição ou exclusão de informações.
10 – Vandalismo / terrorismo	Atos de vandalismo / terrorismo que venha a destruir dependências do data

	center, componentes de comunicação e arquivos físicos.

Comitê de Crise

É responsabilidade deste Comitê, manter o **PAC "plano de administração de crise"** atualizado e decidir pelo seu acionamento quando da ocorrência de desastres, respondendo em nível institucional pela execução do plano e demais ocorrências relacionadas. Inclui autoridades em nível institucional e tomadores de decisão da **Epeople**.

É responsável por todas as comunicações durante um desastre. Especificamente, eles se comunicarão com os funcionários, clientes, autoridades, fornecedores e até mesmo com a mídia, se necessário.

O líder desta equipe administrará e manterá o Plano de Administração de Crise.

EQUIPE DE INSTALAÇÕES/AMBIENTE:

Responsável pelas instalações físicas que abrigam sistemas de TIC e pela garantia que as instalações de alternativa são mantidas adequadamente. Avalia os danos e supervisiona os reparos. O líder desta equipe administrará e manterá o Plano de Recuperação de Desastre.

EQUIPE DE REDES:

Responsável por avaliar os danos específicos de qualquer infraestrutura de rede e para fornecer dados e conectividade de rede, incluindo WAN, LAN ou de infraestrutura externa junto aos prestadores de serviço.

EQUIPE DE INFRAESTRUTURA/APLICAÇÕES:

Responsável por fornecer a infraestrutura de servidor físico e virtuais necessária para que a TI execute suas operações e processos essenciais durante um desastre.

Garantir que as aplicações essenciais funcionem como exigido para atender aos objetivos de negócios em caso de e durante um desastre. Eles serão os principais responsáveis por assegurar e validar o desempenho das aplicações essenciais e podem ajudar outras equipes conforme necessário.

EQUIPE DE OPERAÇÕES:

Responsável por fornecer aos funcionários as ferramentas de que necessitam para desempenhar suas funções da forma mais rápida e eficiente possível. Eles precisarão provisionar todos os funcionários da **Epeople** na solução de contingência e aqueles que trabalham remotamente com as ferramentas específicas à sua atuação.

O líder desta equipe administrará e manterá o Plano de Continuidade Operacional.

EQUIPE DE BACKUP:

Responsável por analisar as perdas e mapear a quantidade de dados perdidos, tempo de recuperação desses dados e formular estratégia de recuperação de dados de acordo com as políticas pré-estabelecidas.

EQUIPE DE SEGURANÇA DA INFORMAÇÃO:

Responsável por prover mecanismos de segurança no ambiente principal e alternativo. Resguardar aplicações e dados, evitando que desdobramentos de segurança afetem o acionamento da continuidade, cuja proteção estará contida na política de segurança.

ACIONAMENTO DO PLANO

Este plano será acionado quando da ocorrência de algum dos cenários de desastres, a insurgência ou ocorrência de um risco desconhecido ou caso uma vulnerabilidade tenha grande possibilidade de ser explorada. O plano também poderá ser invocado em casos de testes ou por determinação da diretoria **Epeople**.

Os integrantes do Comitê de Crise serão responsáveis por acionar os contatos e partes interessadas, prioritariamente por telefone, ou pessoalmente caso seja possível.

Estratégia de Continuidade

A estratégia de continuidade para o cenário atual e serviços essenciais da **Epeople**, está estabelecida pelo fornecedor especializado de serviços de Data Center contratado pela **Epeople**, respeitando os acordos de nível de serviço estabelecidos no contrato.

Plano de Continuidade Operacional (PCO)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos alternativos planejados, definindo as atividades prioritárias para garantir a continuidade dos serviços essenciais.

OBJETIVO E ESCOPO

É escopo deste plano **garantir ações de continuidade durante e depois da ocorrência de uma crise** ou cenário de desastre tratando-se apenas das ações de contingência definidas na estratégia.

SÃO OBJETIVOS PCO:

Prover meios para manter o funcionamento dos principais serviços e a continuidade das operações de TI e dos sistemas essenciais.

Estabelecer procedimentos, controles e regras alternativas que possibilitem a continuidade das operações de TI durante uma crise ou cenário de desastre.

Estabelecer uma equipe para cada plano PCO, PRD e PAC

Definir os formulários, checklists e relatórios a serem entregues pelas equipes ao executar a contingência.

GESTÃO

O fornecedor de serviços de Infraestrutura e Data Center da **Epeople** é a unidade responsável por implementar, manter e melhorar o PCO e toda documentação inerente.

EXECUÇÃO DO PLANO (Avaliação de Impacto de Desastre)

Identificada a ocorrência de um incidente ou crise e o Líder da Equipe de Operação deve verificar a dimensão do impacto, extensão e possíveis desdobramentos do ocorrido. Divulgar a informação a todas as equipes envolvidas.

ACIONAMENTO DO PLANO

Dado o aval pelo Comitê de Crise ao acionamento do plano a Equipe de Infraestrutura da **Epeople** abrirá um incidente e realizará os escalonamentos ao fornecedor de serviços de Data Center que executarão os planos de PRD e PAC com o intuito de:

- ✓ Cumprir os prazos e orquestrar as ações de contingência.
- ✓ Informar as equipes ações de contingência com a priorização dos serviços essenciais.

ENCERRAMENTO DO PCO

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do Data Center deverá ser emitido um parecer relatando as atividades realizadas neste PCO. Informar ao Comitê de Crise o retorno das atividades.

PLANO DE ADMINISTRAÇÃO DE CRISES (PAC)

Este plano especifica as ações ante os cenários de desastres. As ações incluem gerir, administrar, eliminar ou neutralizar os impactos, inerente ao relacionamento entre os agentes envolvidos e/ou afetados, até a superação da crise, através da orquestração das ações e de uma comunicação eficaz.

OBJETIVO

O objetivo deste plano é garantir a comunicação, gerenciar as crises e viabilizar uma compreensão linear a todos os envolvidos das ações antes, durante e após a ocorrência de uma catástrofe.

SÃO OBJETIVOS ESPECÍFICOS DO PAC:

- ✓ Garantir a segurança à vida das pessoas;
- ✓ Minimizar transtornos sobre os desdobramentos de incidente e estimular o esforço em conjunto para superação da crise;
- ✓ Orientar os funcionários e demais colaboradores com informações e procedimentos de conduta; e
- ✓ Informar a sociedade em tempo e com esclarecimentos condizentes com o ocorrido.

EXECUÇÃO DO PLANO (Comunicação na Ocorrência de um Desastre)

Na ocorrência de um desastre será necessário entrar em contato com diversas áreas, principalmente as afetadas para informá-las de seu efeito na continuidade dos serviços e tempo de recuperação. A equipe de comunicação será responsável por contatar estas unidades e passar as informações pertinentes a cada grupo, setor ou seguimento.

A comunicação com cada parte ocorrerá da seguinte forma:

- ✓ Comunicar às autoridades;
- ✓ A prioridade da equipe de comunicação será assegurar que as autoridades competentes tenham sido notificadas da catástrofe, principalmente se envolver risco às pessoas, fornecendo as seguintes informações de localização, natureza, magnitude e impacto do desastre.

Comunicação após um Desastre:

Após reunião do Comitê de Crise, a equipe de comunicação elaborará um breve programa de comunicação para acionar as partes envolvidas e afetadas de modo a manter todos bem informados e passar a todos a perspectiva dos esforços necessários para o restabelecimento dos serviços inativos.

Comunicação com os funcionários:

A equipe de comunicação deverá prover um meio de contato específico para este fim, com intuito de que as unidades da **Epeople** se mantenham informadas da ocorrência de um desastre e da inatividade dos serviços essenciais de TI.

Números de contatos a serem disponibilizados:

Telefone: (DDD) :

Contatos de E-mail:

Central de Serviços (service desk):

*Caso não haja conectividade ou linha telefônica disponível, ceder essas informações por meio de publicações, ou outra estratégia definida no momento.

Comunicar unidades e setores da **Epeople**:

Acionar diretamente às unidades afetadas pelo desastre e fornecer contato. Informar a natureza, o impacto e a abrangência da catástrofe, como também as ações de contingência em andamento.

Comunicar colaboradores externos, cidadãos e mídia:

A equipe de comunicação, em consonância com a comunicação da **Epeople**, deverá fornecer informações pertinentes aos colaboradores externos: advogados, cidadãos e outros órgãos. Buscar publicar em meios oficiais e de ampla divulgação, com aval do Comitê de Continuidade e institucional, informações sobre o ocorrido.

Comunicar o retorno das operações:

Comunicar a todas as partes acima supracitadas quando ocorrer o retorno das operações à normalidade.

ENCERRAMENTO DO PAC

Uma vez validado o funcionamento do retorno dos sistemas essenciais e estabilidade do Data Center a Equipe de Comunicação entrará em contato com as partes descritas neste plano provendo as informações de retorno das operações com as informações de status dos serviços essenciais. Compor relatório com relação das atividades necessárias após a ocorrência do desastre como remanejamento dos canais de informação, abertura e acompanhamento de chamados correlatos ao ocorrido.

PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

Este plano descreve os cenários de inoperância e seus respectivos procedimentos planejados, definindo as atividades prioritárias para restabelecer o nível de operação dos serviços no ambiente afetado dentro de um prazo tolerável.

OBJETIVO E ESCOPO

É escopo deste plano garantir o retorno das operações do ambiente principal depois da ocorrência de uma crise ou cenário de desastre tratando-se apenas dos ativos, conexões e configurações deste ambiente.

São objetivos do PRD:

- ✓ Avaliar danos aos ativos e conexões do Data Center e prover meios para sua recuperação;
- ✓ Evitar desdobramentos de outros incidentes na facilidade principal; e
- ✓ Restabelecer o Data Center dentro do prazo tolerável.

EXECUÇÃO DO PLANO

- ✓ Identificar ativos danificados;
- ✓ As equipes de instalação/backup/servidores/rede deverão identificar e listar todos os ativos danificados da ocorrência do desastre;
- ✓ Identificar acessos interrompidos;
- ✓ A equipe de rede deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando se a abrangência está na rede local, rede WAN ou com o provedor de serviços;
- ✓ Listar serviços descontinuados;
- ✓ A equipe do PRD deverá **mapear quais serviços foram descontinuados** contendo as informações de perda de ativo e de conexão com intuito de levar ao conhecimento do Comitê de "Desaster Recovery". O relatório deverá abranger todos os componentes necessários à plena operação da aplicação como servidores, máquinas virtuais, banco de dados, firewall, storage, routers e switches, bem como respectivas configurações de proxy, dns, rotas, vlans etc.;
- ✓ Elaborar cronograma de recuperação;

- ✓ O líder do PRD após o mapeamento das perdas e impactos elaborará um breve cronograma de recuperação das aplicações levando em consideração:
  - ▪ A priorização dos serviços essenciais, ou determinação de nível institucional;
  - ▪ O tempo de retorno definido para cada serviço essencial; e
  - ▪ A força de trabalho disponível.
- ✓ Substituição de ativos e equipamentos;
- ✓ Em caso de perda de ativos, deverá ser imediatamente informado ao comitê de DR "Desaster Recovery" a necessidade de aquisição de ativos perdidos que não puderem ser recuperados. A equipe irá mensurar quanto tempo a aquisição irá impactar o RTO de cada serviço comunicando ao CDR se há alguma solução alternativa a ser tomada enquanto é realizada a aquisição.
- ✓ A equipe de instalações deve verificar quais ativos foram danificados estão cobertos por garantia e se poderá ser acionada neste caso através dos fornecedores;
- ✓ As informações pertinentes à alteração do tempo de recuperação dos serviços serão passadas às equipes do PCO e PAC;
- ✓ Reconfiguração de ativos e equipamento; e
- ✓ A equipe de instalações deverá verificar que as configurações dos ativos reparados ou substituídos estão em funcionamento pleno. Caso não estejam, prover cronograma estimado para configurar estes ativos informando à equipe de comunicação e CDR "Comitê de Crise".

TESTE DE AMBIENTE

O ambiente principal do Data Center antes do recovery dos dados do backup deverá ser testado a fim de garantir que o processo de recuperação ocorra conforme o planejado. Os testes incluem:

- ✓ Garantir os mesmos níveis de capacidade e disponibilidade dos serviços essenciais antes do desastre;
- ✓ Recuperar dados do backup;
- ✓ Proceder a recuperação dos dados para as aplicações, seja do storage ou fitas de backup;
- ✓ Validar as configurações e funcionalidades dos sistemas. A validação pode ser realizada pelos testes automatizados de monitoramento dos serviços por equipe designada pela equipe de configuração dos sistemas .

ENCERRAMENTO DO PRD

Ao término do procedimento de recuperação, as informações serão consolidadas em parecer específico informando horário de restabelecimento de cada serviço, equipamentos adquiridos, procedimentos de recuperação realizados e fornecedores acionados.

DOCUMENTO DE VALIDAÇÃO E TESTE

O PT "Plano de Testes" será executado e validado através de checklist em reunião entre os líderes de cada equipe a cada semestre ou com a insurgência de novos fatores de risco, mudança na análise de impacto, ou com a inclusão de um novo serviço no plano de continuidade.