



PCN - Plano de Continuidade Infraestrutura BPO Saúde e Data Center

Sumário

1. CAMPO DE APLICAÇÃO	4
2. ABRANGÊNCIA.....	4
3. DEFINIÇÕES.....	4
4. DIRETRIZES.....	5
5. DIRETRIZES DO PLANO	5
6. RESPONSABILIDADES.....	8
7. PLANO DE GERENCIAMENTO DE RISCOS.....	10
8. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO DATACENTER BENNERCLOUD – ORACLE OCI.....	12
9. QUANTIFICAÇÃO DOS RISCOS	13
10. PLANO DE AÇÃO PARA CONTIGÊNCIA.....	16
11. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO INFRAESTRUTURA BPO SAÚDE ALPHAVILLE.....	23
12. QUANTIFICAÇÃO DOS RISCOS	24
13. PLANO DE AÇÃO PARA CONTIGÊNCIA.....	27
14. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO INFRAESTRUTURA BPO SAÚDE MARINGÁ.....	33
15. QUANTIFICAÇÃO DOS RISCOS	34
16. PLANO DE AÇÃO PARA CONTIGÊNCIA.....	36
17. RESPONSABILIDADE DE ATIVAÇÃO E EXECUÇÃO.....	43
18. CONTATO FONECEDORES E PARCEIROS	43

19. PLANO DE AÇÃO PREVENTIVO, MONITORAMENTO E CONSCIENTIZAÇÃO	44
20. ELIGIBILIDADE E VALIDADE	45
21. REGISTRO DE ALTERAÇÕES.....	45
22. FORMALIZAÇÃO	45

1. CAMPO DE APLICAÇÃO

O Plano de Continuidade de Negócios tem por objetivo definir estratégia da Plano de recuperação dos serviços Bennercloud e operação BPO Saúde quanto a disponibilidade de infraestrutura, bem como os papéis e responsabilidade que irão garantir a sustentação dos planos.

2. ABRANGÊNCIA

Este plano abrange os serviços e clientes do Datacenter Bennercloud e BPO Saúde.

3. DEFINIÇÕES

- **Ataque Cibernético** - Ação maliciosa realizada por meio da rede ou sistemas de informação com o objetivo de comprometer ou interromper a confidencialidade, integridade ou disponibilidade dos ativos de informação.
- **Evento** – Acontecimento interno ou externo, que pode gerar ou não impacto físico ou lógico sobre a operação Bennercloud e BPO Saúde.
- **Emergência** – Evento que se materializou explorando uma vulnerabilidade física que gera impacto direto sobre os serviços e ativos.
- **Crise** – Cenário avançado de um incidente ou emergência que não foi possível ser tratado pelos planos de resposta estruturados.
- **Desastre** – Cenário de materialização de uma crise, sendo difícil mensurar a dimensão de todos os impactos gerados ao negócio e pessoas.
- **Incidente** – Situação que pode representar ou levar a interrupção de negócios, perdas, emergências ou crises.
- **MDR** - Managed Detection and Response ou Detecção e Resposta Gerenciadas, em português, é uma solução de segurança cibernética que oferece detecção proativa de ameaças, monitoramento e capacidades de resposta, combinadas com a análise de dados e equipe de especialistas em segurança formada por caçadores de ameaças e atendentes a incidentes em segurança cibernética.
- **Restauração** – Momento estratégico de acionamento dos planos de continuidade Bennercloud que possuem o objetivo de retornar à operação a partir do site principal.

- **Recuperação** – Momento estratégico de acionamento dos planos de continuidade Bennercloud que possuem o objetivo de habilitar novamente a operação para operar em um site alternativo ou por meio de contingência sem impactar o negócio.
- **BIA** – Análise de Impacto no Negócio. Descreve os impactos que a operação pode sofrer devido a interrupção de um ou mais processos ou serviços.
- **PRD** – Plano de Recuperação de Desastres, orienta e suporta as atividades de entrada e operação em contingência da área de TI e a infraestrutura tecnológica envolvida.

4. DIRETRIZES

As diretrizes de Plano de Continuidade Bennercloud e BPO Saúde estão estabelecidas a partir de um ciclo de gestão e gerenciamento:

- Entender a operação
- Selecionar Opções de Continuidade dos Negócios
- Implementar uma resposta de Continuidade dos Negócios e Serviços

5. DIRETRIZES DO PLANO

5.1 – Entender o Plano

5.1.1 – Planejar a revisão do PCN

- Realizar o Planejamento do PCN e identificar os novos cenários de continuidade dos negócios. Este estudo deve ocorrer sempre que necessário e conter as atividades referente a PCN que serão praticadas. Essa revisão anual deve contemplar todas as etapas abaixo.

5.1.2 – Conduzir a Análise de Impacto nos Negócios

- O BIA deve sempre considerar dependências externas e internas dos processos de negócio, na visão de serviços de negócio.
- O BIA deve analisar o impacto financeiro, de imagem e legal em relação aos tempos de parada, respeitando os critérios estabelecidos na Política de Gestão de Riscos do Bennercloud e operação BPO Saúde.

- Os processos de negócio mais críticos devem ser claramente identificados e priorizados por TMR (tempo máximo de retorno).
- Devem ser claramente identificados os recursos necessários em contingência por área/processo de negócio e serviços.
- Os tempos máximos de indisponibilidade devem ser obtidos juntamente com as áreas de negócio e validado com seus respectivos clientes.

5.1.3 – Conduzir avaliação de riscos

- A avaliação de Riscos deve possuir escopo definido, abordando aspectos relacionados à continuidade dos negócios como estrutura e segurança física, dependência de terceiros, dependência de colaboradores e sistemas.
- A avaliação de Riscos deve possuir mapeamento detalhado dos riscos, considerando as ameaças potenciais e respectivos graus de vulnerabilidade.
- A avaliação de riscos deve avaliar os cenários de riscos que a Organização esteja exposta, desta forma orientando as estratégias de recuperação.

5.2 – Determinar estratégias de continuidade dos negócios

- A estratégia de continuidade deverá ser definida levando em consideração a priorização dos processos críticos de negócio e as principais exposições a riscos da operação.
- Deverão ser documentadas todas as modificações de infraestrutura nas áreas de negócios, que originará o Relatório de Estratégia de Continuidade.
- Os relatórios gerados neste processo deverão possuir estimativa de custos e planos de implementação, definidos com apoio das áreas responsáveis e deverão ser aprovados pelo comitê.
- Sempre que for definida uma nova estratégia de continuidade esta deve ser submetida à aprovação.

5.3 – Implementar uma resposta de continuidade dos negócios

- Os documentos de suporte à resposta a incidentes (Plano de Recuperação de Desastres, e Plano de Análise de Risco) deverão ser confeccionados, em conjunto com as áreas responsáveis pela sustentação do ambiente, equipe do Datacenter, BPO Saúde e Cliente, para

obter o melhor resultado e de acordo com a implementação das estratégias de continuidade dos negócios e de TI e com as diretrizes estabelecidas na fase de Planejamento.

- Estes documentos deverão ficar disponíveis em locais de fácil acesso a todos os envolvidos na PCN, de forma que seja possível acessá-los sempre que necessário. O armazenamento destes documentos deve considerar inclusive cenários de interrupção nos serviços de tecnologia, como indisponibilidade de servidores. Dessa forma, recomenda-se manter vias impressas desses documentos em mais de um local.
- O Plano de Recuperação de Desastre deve conter o escopo, responsáveis e propósito definidos e as atividades que devem ser executadas dependendo do cenário de indisponibilidade.
- O Plano de Recuperação de Desastre deve conter o detalhamento das atividades necessárias para recuperação dos sistemas, contemplando o passo a passo das atividades de operação das estratégias de recuperação dos sistemas de informação e infraestrutura tecnológica.
- O Plano de Análise de Risco deve conter o grau do impacto, risco, fatores que possam comprometer os serviços, impacto financeiro, de imagem em que um incidente possa causar.

5.4 – Executar e testar a resposta a incidentes

- Em caso de incidentes críticos de qualquer natureza, os procedimentos de resposta deverão ser aqueles disponíveis nos documentos de suporte à resposta a incidentes;
- Os testes dos procedimentos descritos nos documentos de suporte à resposta a incidentes deverão ser realizados de acordo com a periodicidade.
- Durante a realização de um teste, para cada procedimento avaliado e revisado no plano.

5.5 – Competência e conscientização

5.5.1 – Desenvolver programas de conscientização PCN

- A partir do cronograma definido no processo de planejamento da PCN, a área responsável pela Plano de Continuidade dos Negócios deverá realizar treinamentos de modo a conscientizar todos os envolvidos sobre seus papéis e responsabilidades diante da PCN e

segurança da informação, bem como sobre o funcionamento básico dos procedimentos de resposta a incidentes.

6. RESPONSABILIDADES

6.1. Diretoria Executiva

- Designar e atribuir responsabilidade pela Coordenação da Gestão da Continuidade do Negócio;
- Certificar-se que a Gestão da Continuidade do Negócio está adequada as necessidades da empresa e/ou negócio;
- Garantir os recursos necessários para a manutenção da Gestão da Continuidade do Negócio;
- Deliberar sobre assuntos estratégicos no Gerenciamento de Incidentes;
- Garantir a execução das respostas a um incidente.

6.2. Comissão de Resposta a Incidentes

- Determinar o momento de acionamento de cada área relacionada;
- Centralizar as ações e esforços para recuperação e restauração dos ambientes impactados, visando acelerar o processo de tomada de decisão e alinhamento de atividades;
- Acompanhar e realizar escalonamento sempre que necessário para atendimento das necessidades das áreas de negócio e tecnologia

6.3. Gestão de Riscos

- Avaliar periodicamente os critérios para a criação de novos Planos de Continuidade do Negócio e manutenção dos existentes;
- Determinar as abordagens necessárias para a realização das avaliações de impacto e riscos ao negócio;
- Incluir novos Planos de Continuidade do Negócio sempre que for detectada sua necessidade;
- Apoiar a comunicação entre as equipes de continuidade e gestores;
- Garantir que os requisitos regulamentares estão sendo atendidos pelos Planos de Continuidade do Negócio;

- Apoiar a comunicação de retomada;
- Gerenciar o Sistema de Gestão da Continuidade do Negócio - bem como definir os prazos de manutenção dos planos;
- Criar e manter a documentação de continuidade do negócio;
- Promover a Gestão da Continuidade no Bennercloud e operação BPO Saúde;
- Apoiar e acompanhar o desenvolvimento dos treinamentos e campanhas de continuidade do negócio aos envolvidos;
- Desenvolver as atividades deliberadas pelo Comitê de Gestão de Crises;
- Gerenciar toda a resposta, retomada, recuperação e atividades de restauração da operação.

6.4. TI / DC

- Gerenciar e atualizar os Planos de Recuperação de Desastres sempre que houver alterações como, equipamento ou alguma outra alteração de nível operacional, troca de funcionários da área ou criação de novos procedimentos de trabalho, ou quando for verificada alguma inconformidade por meio de testes;
- Atualizar e gerenciar procedimentos e tarefas das equipes que suportam os serviços de TI em ambiente de contingência;
- Executar testes dos Planos de Recuperação de Desastres de TI de acordo com as demandas da operação;
- Atuar com foco na garantia da alta disponibilidade dos ambientes críticos do Bennercloud e BPO Saúde;
- Atuar proativamente como agente de riscos, apoiando e alimentando os processos de Gestão de Riscos do Bennercloud e BPO Saúde, visando minimizar a exposição da operação a eventos que comprometam a disponibilidade, confidencialidade e integridade das informações;
- Assegurar que o desenvolvimento e/ou implantação de novos sistemas e ambientes de TI sempre sejam avaliados em aspectos de continuidade da operação;
- Atuar proativamente com foco na otimização de custos e recursos do Bennercloud e BPO Saúde, no que se refere às estratégias de Continuidade Operacional e Negócios;

- Garantir o cumprimento de requisitos (infraestrutura) contratuais do Bennercloud e BPO Saúde com prestadores de serviços, terceiros, no que se refere às estratégias de Continuidade de Negócios.

7. PLANO DE GERENCIAMENTO DE RISCOS

7.1. Processo de Gerência De Riscos

- Serão considerados os riscos inicialmente identificados pela equipe do projeto;
- Caso sejam encontrados novos riscos no decorrer do desenvolvimento do projeto, estes deverão ser descritos neste documento;
- As respostas possíveis aos riscos serão decididas entre os gerentes do projeto mediante a aprovação do gerente de projetos;
- A identificação dos riscos será feita através de uma os membros da equipe do projeto.

7.2. Identificação dos Riscos

Riscos Considerados		
Riscos não técnicos	Riscos Legais	Riscos Técnicos
Prazos	Contratos	Obsolescência
Custos	Satisfação	Desempenho
Recursos Humanos	Legal / LGPD	Indisponibilidade
Processos e Sistemas		

De acordo com as etapas definidas na Estrutura Analítica do Projeto, seguem abaixo os riscos identificados:

7.3. Qualificação e Impacto dos Riscos

Grau de Impacto	Peso
Muito Grande	5
Grande	4
Moderado	3
Pequeno	2
Muito Pequeno	1

Muito Grande - O impacto é extremamente elevado, sendo necessária uma interferência direta, imediata e precisa da equipe do projeto, para que os resultados não sejam seriamente comprometidos;

Grande - Impacto de maior relevância, necessitando de um gerenciamento mais preciso, podendo prejudicar os resultados;

Moderado - Impacto considerado relevante, necessitando uma maior atenção em sua análise e resolução, oferecendo risco moderado aos resultados;

Pequeno - O impacto pequeno, em termos de custos ou prazos, fácil solução;

Muito Pequeno - Impacto quase que irrelevante, de fácil solução;

7.4. Avaliação da Probabilidade

Referencial	Probabilidade
Grande chance de ocorrer	1.0
Provavelmente ocorrerá	0.75
Igual chance de ocorrer ou não	0.5
Baixa chance de ocorrer	0.25
Pouca chance de ocorrer	0.1

Grande chance de ocorrer - a probabilidade de ocorrência é iminente (maior que 80%).

Provavelmente ocorrerá - probabilidade importante de ocorrer (de 60 a 80%).

Igual chance de ocorrer ou não - probabilidade razoável de ocorrer (de 40 a 60%).

Baixa chance de ocorrer - probabilidade baixa de ocorrência (de 20 a 40%).

Pouca chance de ocorrer - probabilidade quase que imperceptível (menor que 20%).

7.5. Matriz de Probabilidade x Impacto

	Impacto					
Probabilidade		1.0	2.0	3.0	4.0	5.0
1.0		1	2	3	4	5
0.75		0.75	1.5	2.25	3	3.75
0.5		0.5	1	1.5	2	2.5
0.25		0.25	0.5	0.75	1	1.25
0.1		0.1	0.2	0.3	0.4	0.5

8. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO

DATACENTER BENNERCLOUD – ORACLE OCI

A Oracle OCI é uma plataforma segura e confiável, que possui diversas certificações e atende a padrões rigorosos de segurança e disponibilidade, tais como Certificações SOC 1/SOC 2/SOC 3, ISO 27001, PCI DSS e HIPAA. Todos os serviços do cliente estão disponíveis em servidores redundantes e com alta disponibilidade.

É importante destacar que adotamos um compromisso sólido com a segurança, disponibilidade e confiabilidade em nossas operações. Fazemos uma gestão de vulnerabilidade ativa, com avaliações diárias de vulnerabilidade e aplicação semanal de correções de segurança em nossos equipamentos e servidores. Essa abordagem proativa garantir a solidez e a resiliência de nosso ambiente tecnológico.

Link de Internet Datacenter				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade dos serviços	0.1	5	0.5
Serviço de DNS				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade de acesso aos serviços	0.1	0.25	0.25
Servidores Virtuais				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	0.1	0.1
Serviços de rede				
Seq.	Evento	Probabilidade	Impacto	Matriz
	VCN	0.25	2	0.5
Servidores Banco de Dados				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	0.1	0.1
Ataques Cibernéticos				

Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual e indisponibilidade	0.25	5	1.25

9. QUANTIFICAÇÃO DOS RISCOS

Link de Internet Datacenter	
Tempo do atraso por evento	0 Hora
Frequência no período	Não houve eventos nos últimos 12 meses
Total atraso no período	Não houve eventos nos últimos 12 meses
Fatores considerados (Diretos)	<ul style="list-style-type: none">- Indisponibilidade de serviços- Multa contratual- SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none">- Imagem da empresa- Insatisfação do Cliente
Probabilidade de ocorrência	0.5

Serviço de DNS	
Tempo do atraso por evento	0 Hora
Frequência no período	Não houve eventos nos últimos 12 meses
Total atraso no período	Não houve eventos nos últimos 12 meses
Fatores considerados (Diretos)	<ul style="list-style-type: none">- Indisponibilidade total ou parcial nos acessos aos serviços- SLA- Multa contratual
Fatores considerados (Indiretos)	<ul style="list-style-type: none">- Imagem da empresa- Insatisfação do Cliente

Probabilidade de ocorrência	0.25
-----------------------------	------

Servidores Virtuais	
Tempo do atraso por evento	30 minutos
Frequência no período	1x ano
Total atraso no período	30 Minutos
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade do serviço - Possibilidade de Perda de dados - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente - SLA com Clientes
Probabilidade de ocorrência	0.5

Serviços de rede	
Tempo do atraso por evento	Não houve eventos nos últimos 12 meses
Frequência no período	Não houve eventos nos últimos 12 meses
Total atraso no período	Não houve eventos nos últimos 12 meses
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade parcial dos serviços - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente
Probabilidade de ocorrência	0.5

Servidores de Banco de Dados	
Tempo do atraso por evento	30 minutos
Frequência no período	1x ano
Total atraso no período	30 minutos
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade parcial dos serviços - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente
Probabilidade de ocorrência	0.5

Ataques Cibernéticos	
Tempo do atraso por evento	Não houve eventos nos últimos 12 meses
Frequência no período	Não houve eventos nos últimos 12 meses
Total atraso no período	Não houve eventos nos últimos 12 meses
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade total ou parcial dos serviços - Comprometimento do SLA com Clientes - Indisponibilização ou perda de dados - Retrabalho (reconfiguração de servidores)
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente - Comunicação aos órgãos competentes

	- Questões jurídicas
Probabilidade de ocorrência	1.25

10. PLANO DE AÇÃO PARA CONTIGÊNCIA

Na ocorrência do incidente que afete as informações, este plano de contingência deverá ser ativado de modo a garantir a continuidade dos serviços. Além do plano de continuidade, a operação mantém uma lista de mitigações de forma a minimizar os danos que venham a ocorrer no caso de incidente.

Evento	
Link Internet Datacenter	
Descrição	
Ocorre quando a comunicação da rede WAN é interrompida com a rede local LAN, impossibilitando assim a comunicação entre os clientes e o Datacenter ou serviços.	
Informações adicionais	
Gatilho	Aguardar 30 minutos antes de acionar a contingência
Tempo de Recuperação	TMP = 30 minutos
Desejável	NMD = 50%
	TMR = 2 horas
TMP = Tempo Máximo de parada, até que a atividade reinicie.	
NMD = Nível Mínimo de desempenho da atividade após reinício.	
TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e suporte
Benner Datacenter	Verificar o problema na redundância de conectividade; Abrir um chamado na Oracle OCI;

	Validar os dispositivos de conectividade e rede; Se houver um falhar na região, acionar o plano de recuperação do serviço migrando para a região vinhedo; Acionar o processo de chaveamento (manual ou automático) para a segunda região da Oracle.
RTO	2 horas
RPO	N/A
Evento	
DNS	
Descrição	
Ocorre quando o acesso é negado ou não é possível a resolução do nome do serviço para acesso.	
Informações adicionais	
Gatilho	Aguardar 30 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 50% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Se o incidente for apenas para o ambiente do cliente, a comunicação será pontual e para o cliente. Para incidente geral, acionar o plano de comunicação geral aos clientes do Datacenter.
Benner Datacenter	Verificar o problema no serviço Oracle no painel; Abrir um chamado na Oracle OCI; Se for um incidente isolado o DNS do cliente, recriar a publicação Se houver um falhar na região, acionar o plano de recuperação do serviço; Acionar o processo de chaveamento (manual ou automático) para a segunda região da Oracle.

RTO	1 hora
RPO	N/A

Evento	
Servidores Virtuais	
Descrição	
Ocorre quando um servidor apresenta problemas lógicos (corrompido), impossibilitando seu correto funcionamento e acesso, inviabilizando o retorno da operação quanto aos serviços hospedados.	
Informações adicionais	
Gatilho	Aguardar 30 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 50% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Se o incidente for apenas para o ambiente do cliente, a comunicação será pontual e para o cliente. Para incidente geral, acionar o plano de comunicação geral aos clientes do Datacenter.
Benner Datacenter	Verificar o problema no servidor virtual; Abrir um chamado no Datacenter; Se for um incidente isolado no servidor, solicitar a reparação ou retorno de backup via <i>bucket</i> ;

	<p>Se houver um falhar na região, acionar o plano de recuperação do serviço;</p> <p>Acionar o processo de chaveamento (manual ou automático) para a segunda região da Oracle.</p>
RTO	1 hora
RPO	<p>Para máquinas virtuais de aplicação 7 dias.</p> <p>Para serviço de Banco de Dados ou Arquivos. Máximo 1 hora.</p>

Evento	
Serviços de Rede	
Descrição	
Ocorre quando o acesso a rede LAN está indisponível total ou parcial aos usuários de forma simultânea, impossibilitando qualquer acesso aos serviços da rede local como servidores, compartilhamentos, publicações e outros.	
Informações adicionais	
Gatilho	Aguardar 30 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	<p>TMP = 30 minutos</p> <p>NMD = 50%</p> <p>TMR = 1 hora</p>
<p>TMP = Tempo Máximo de parada, até que a atividade reinicie.</p> <p>NMD = Nível Mínimo de desempenho da atividade após reinício.</p> <p>TMR = Tempo Máximo de retomada dos níveis normais de operação</p>	
Contingência	
Benner	<p>Informar imediatamente a equipe de TI. Iniciar o protocolo de comunicação com os clientes sobre a interrupção do serviço.</p> <p>Preparar canais de suporte ao cliente para aumento de demanda.</p>
Benner Datacenter	<p>Abrir um atendimento com a Oracle OCI;</p> <p>Validar Máquina Virtual Movida para outro FD ou região;</p>

	Ajustes no DNS; Validar o monitoramento da LAN e Conectividade entre os servidores e serviços.
RTO	1 hora
RPO	N/A

Evento	
Servidores de Banco de Dados	
Descrição	
Falha crítica nos servidores de banco de dados, resultando em perda de acesso aos dados e serviços críticos.	
Informações adicionais	
Gatilho	Deteção de inatividade nos servidores de banco de dados ou alertas críticos de monitoramento de sistema.
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 60% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar imediatamente a equipe de TI. Iniciar o protocolo de comunicação com os clientes sobre a interrupção do serviço. Preparar canais de suporte ao cliente para aumento de demanda.
Benner Datacenter	Verificar imediatamente a integridade dos servidores de banco de dados. Se necessário, ativar servidores de backup através do backup do <i>bucket</i> . Investigar a causa da falha e iniciar reparos. Restaurar os dados a partir do backup mais recente.
RTO	1 hora
RPO	Até 1 hora

Evento	
Ataques Cibernéticos	
Descrição	
Ataques maliciosos originados na rede ou nos sistemas de informação com o objetivo de comprometer ou interromper serviços, roubar dados confidenciais ou corromper informações. Podem ter diversas origens como phishing, ransomware, DDoS, exploits etc.	
Informações adicionais	
Gatilho	Quando há identificação de atividade suspeita pelo time de MDR, onde não foi possível a contenção automatizada.
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 60% TMR = 6 horas
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar imediatamente a equipe de TI. Iniciar o protocolo de comunicação com os clientes sobre a interrupção do serviço. Preparar canais de suporte ao cliente para aumento de demanda.
Benner Datacenter	Verificar imediatamente a integridade dos servidores de banco de dados. Se necessário, ativar servidores de backup através do backup do <i>bucket</i> . Investigar a causa da falha e iniciar reparos. Restaurar os dados a partir do backup mais recente.
RTO	6 horas
RPO	Para máquinas virtuais de aplicação 7 dias. Para serviço de Banco de Dados ou Arquivos. Máximo 1 hora.

11. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO INFRAESTRUTURA BPO SAÚDE ALPHAVILLE

Link de Internet				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade dos serviços	0.25	5	1.25
Interrupção do Serviço de Telefonia - VoIP				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade de acesso aos serviços	0.25	3	0.75
Servidores Virtuais				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.5	3	1.5
Firewall				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	5	0.5
Switches/Access Points				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	3	0.3
Estações de trabalho				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano físico ou lógico	1	0.1	0.75

12. QUANTIFICAÇÃO DOS RISCOS

Link de internet	
Tempo do atraso por evento	4 horas
Frequência no período	2 eventos nos últimos 12 meses
Total atraso no período	8 horas
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade de serviços - Multa contratual - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa; - Insatisfação do Cliente;
Probabilidade de ocorrência	0.25

Interrupção do Serviço de Telefonia - VoIP	
Tempo do atraso por evento	1 hora
Frequência no período	1x nos últimos 12 meses
Total atraso no período	1 hora
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade em acesso aos serviços - SLA - Multa contratual
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa; - Insatisfação do Cliente;
Probabilidade de ocorrência	0.25

Servidores virtuais	
Tempo do atraso por evento	2 horas
Frequência no período	2x nos últimos 12 meses
Total atraso no período	4 horas
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade do serviço - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente - SLA com Clientes
Probabilidade de ocorrência	0.5

Firewall	
Tempo do atraso por evento	Não temos registro
Frequência no período	Não temos registro
Total atraso no período	Não temos registro
Fatores considerados (Diretos)	<ul style="list-style-type: none"> - Indisponibilidade do serviço - SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none"> - Imagem da empresa - Insatisfação do cliente
Probabilidade de ocorrência	0.1

Switches/Access Points	
Tempo do atraso por evento	Não temos registro
Frequência no período	Não temos registro
Total atraso no período	Não temos registro
Fatores considerados (Diretos)	- Possibilidade de indisponibilidade do serviço
Fatores considerados (Indiretos)	- N/A
Probabilidade de ocorrência	0.1

Estações de trabalho	
Tempo do atraso por evento	Não temos registro
Frequência no período	Não temos registro
Total atraso no período	Não temos registro
Fatores considerados (Diretos)	- N/A
Fatores considerados (Indiretos)	- N/A
Probabilidade de ocorrência	0.75

13. PLANO DE AÇÃO PARA CONTINGÊNCIA

Na ocorrência do incidente que afete as informações, este plano de contingência deverá ser ativado de modo a garantir a continuidade dos serviços. Além do plano de continuidade, a operação mantém uma lista de mitigações de forma a minimizar os danos que venham a ocorrer no caso de incidente.

Evento	
Link Internet ou conectividade	
Descrição	
Ocorre quando a comunicação da rede WAN é interrompida com a rede local LAN, impossibilitando assim a comunicação entre os clientes e o Datacenter ou serviços.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 20 minutos NMD = 75% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e suporte Verificar o problema na conectividade do link; Ativar link de contingência; Abrir ticket na operadora com falha;
RTO	20 minutos
RPO	N/A

Evento	
Interrupção do Serviço de Telefonia - VoIP	
Descrição	
Ocorrência de falhas na comunicação via VoIP, afetando ligações internas e externas.	
Informações adicionais	
Gatilho	N/A
Tempo de Recuperação Desejável	TMP = Conforme SLA contratado. NMD = 30% de chamadas processadas com sucesso. TMR = Conforme capacidades técnicas e SLA contratado.
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Ativar a conexão de internet redundante para manter o serviço de VoIP operacional. Informar os clientes por canais de atendimento e suporte; Abrir um ticket de suporte com o provedor do serviço de VoIP ou com o provedor de internet para a resolução do problema.
RTO	N/A
RPO	N/A

Evento	
Servidores Virtuais	
Descrição	
Ocorre quando um servidor apresenta problemas físicos ou lógicos (corrompido), impossibilitando seu correto funcionamento e acesso, inviabilizando o retorno da operação quanto aos serviços hospedados.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 15 minutos NMD = 80% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Caso o problema gerar indisponibilidade, informar os clientes por canais de atendimento e suporte; Verificar o problema no servidor virtual; Se for um incidente isolado no servidor, solicitar a reparação ou retorno de backup;
RTO	1 hora
RPO	7 dias

Evento	
Firewall	
Descrição	
Ocorre quando um dos dois equipamentos de firewall interrompe os seus serviços, indisponibilizando o acesso e controle à internet.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 60% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e e-mail Avaliar/verificar o incidente com o firewall ativo; Ativar o firewall contingência; Abrir chamado com fornecedor para avaliar causa e corrigir o firewall problemático;
RTO	1 hora
RPO	N/A

<i>Evento</i>	
Switches / Access Points	
Descrição	
Ocorre quando um dos equipamentos de rede, switches ou access points, apresentam falha e interrompem o funcionamento correto.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 75% TMR = 2 horas
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e e-mail, caso houver impacto na operação; Avaliar/verificar o incidente com o equipamento de rede problemático; Substituir o equipamento problemático caso necessário;
RTO	2 horas
RPO	N/A

<i>Evento</i>	
Estações de trabalho	
Descrição	
Ocorre quando uma estação de trabalho apresenta falha, seja de hardware ou software, interrompendo o funcionamento correto.	
Informações adicionais	
Gatilho	Imediato
Tempo de Recuperação Desejável	TMP = 1 hora NMD = 75% TMR = 2 horas
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Avaliar/verificar o incidente com o equipamento de estação de trabalho problemático; Caso o problema for de hardware, substituir o periférico problemático; Caso o problema for de software, avaliar a situação e, se necessário, reinstalar o aplicativo problemático.
RTO	2 horas
RPO	N/A

14. RELACIONAMENTO DOS EVENTOS X PROBABILIDADE X IMPACTO INFRAESTRUTURA BPO SAÚDE MARINGÁ

Link de Internet				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade dos serviços	0.25	5	1.25
Interrupção do Serviço de Telefonia - VoIP				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Indisponibilidade de acesso aos serviços	0.25	3	0.75
Servidores Virtuais				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.5	3	1.5
Firewall				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	5	0.5
Switches/Access Points				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	0.1	3	0.3
Estações de trabalho				
Seq.	Evento	Probabilidade	Impacto	Matriz
	Dano lógico/virtual	1	1	0.1

15. QUANTIFICAÇÃO DOS RISCOS

Link de internet	
Tempo do atraso por evento	2 horas
Frequência no período	2 eventos nos últimos 12 meses
Total atraso no período	4 horas
Fatores considerados (Diretos)	<ul style="list-style-type: none">- Indisponibilidade de serviços- Multa contratual- SLA com Clientes
Fatores considerados (Indiretos)	<ul style="list-style-type: none">- Imagem da empresa;- Insatisfação do Cliente;
Probabilidade de ocorrência	0.25

Interrupção do Serviço de Telefonia - VoIP	
Tempo do atraso por evento	2 horas
Frequência no período	1x nos últimos 12 meses
Total atraso no período	2 horas
Fatores considerados (Diretos)	<ul style="list-style-type: none">- Indisponibilidade em acesso aos serviços- SLA- Multa contratual
Fatores considerados (Indiretos)	<ul style="list-style-type: none">- Imagem da empresa;- Insatisfação do Cliente;
Probabilidade de ocorrência	0.25

Servidores virtuais	
Tempo do atraso por evento	2 horas
Frequência no período	2x nos últimos 12 meses
Total atraso no período	4 horas
Fatores considerados (Diretos)	- Indisponibilidade do serviço - SLA com Clientes
Fatores considerados (Indiretos)	- Insatisfação do cliente - SLA com Clientes
Probabilidade de ocorrência	0.5

Firewall	
Tempo do atraso por evento	1 hora
Frequência no período	1x nos últimos 12 meses
Total atraso no período	1 hora
Fatores considerados (Diretos)	- Indisponibilidade do serviço - Pode comprometer o SLA com Clientes em casos de longa duração
Fatores considerados (Indiretos)	- Insatisfação do cliente e perda do SLA
Probabilidade de ocorrência	0.1

Switches/Access Points	
Tempo do atraso por evento	Não temos registro
Frequência no período	Não temos registro
Total atraso no período	Não temos registro
Fatores considerados (Diretos)	- Indisponibilidade do serviço
Fatores considerados (Indiretos)	N/A
Probabilidade de ocorrência	0.1

Estações de trabalho	
Tempo do atraso por evento	2 horas
Frequência no período	5
Total atraso no período	10
Fatores considerados (Diretos)	N/A
Fatores considerados (Indiretos)	N/A
Probabilidade de ocorrência	0.25

16. PLANO DE AÇÃO PARA CONTIGÊNCIA

Na ocorrência do incidente que afete as informações, este plano de contingência deverá ser ativado de modo a garantir a continuidade dos serviços. Além do plano de continuidade, a operação mantém uma lista de mitigações de forma a minimizar os danos que venham a ocorrer no caso de incidente.

Evento	
Link Internet ou conectividade	
Descrição	
Ocorre quando a comunicação da rede WAN é interrompida com a rede local LAN, impossibilitando assim a comunicação entre os clientes e o Datacenter ou serviços.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 85% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e suporte Verificar o problema na conectividade do link; Ativar link de contingência; Abrir ticket na operadora com falha;
RTO	30 minutos
RPO	N/A

<i>Evento</i>	
Interrupção do Serviço de Telefonia - VoIP	
Descrição	
Ocorrência de falhas na comunicação via VoIP, afetando ligações internas e externas.	
Informações adicionais	
Gatilho	N/A
Tempo de Recuperação Desejável	TMP = Conforme SLA contratado. NMD = 30% de chamadas processadas com sucesso. TMR = Conforme capacidades técnicas e SLA contratado.
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Ativar a conexão de internet redundante para manter o serviço de VoIP operacional. Informar os clientes por canais de atendimento e suporte; Abrir um ticket de suporte com o provedor do serviço de VoIP ou com o provedor de internet para a resolução do problema.
RTO	N/A
RPO	N/A

Evento	
Servidores Virtuais	
Descrição	
Ocorre quando um servidor apresenta problemas físicos ou lógicos (corrompido), impossibilitando seu correto funcionamento e acesso, inviabilizando o retorno da operação quanto aos serviços hospedados.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 15 minutos NMD = 80% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Caso o problema gerar indisponibilidade, informar os clientes por canais de atendimento e suporte; Verificar o problema no servidor virtual; Se for um incidente isolado no servidor, solicitar a reparação ou retorno de backup;
RTO	1 hora
RPO	7 dias

Evento	
Firewall	
Descrição	
Ocorre quando um dos dois equipamentos de firewall interrompe os seus serviços, indisponibilizando o acesso e controle à internet.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 80% TMR = 1 hora
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e e-mail Avaliar/verificar o incidente com o firewall ativo; Ativar o firewall contingência; Abrir chamado com fornecedor para avaliar causa e corrigir o firewall problemático;
RTO	1 hora
RPO	N/A

Evento	
Switches / Access Points	
Descrição	
Ocorre quando um dos equipamentos de rede, switches ou access points, apresentam falha e interrompem o funcionamento correto.	
Informações adicionais	
Gatilho	Aguardar 10 minutos antes de acionar a contingência
Tempo de Recuperação Desejável	TMP = 30 minutos NMD = 65% TMR = 2 horas
TMP = Tempo Máximo de parada, até que a atividade reinicie. NMD = Nível Mínimo de desempenho da atividade após reinício. TMR = Tempo Máximo de retomada dos níveis normais de operação	
Contingência	
Benner	Informar os clientes por canais de atendimento e e-mail, caso houver impacto na operação; Avaliar/verificar o incidente com o equipamento de rede problemático; Substituir o equipamento problemático caso necessário;
RTO	2 horas
RPO	N/A

<i>Evento</i>	
Estações de trabalho	
Descrição	
Ocorre quando uma estação de trabalho apresenta falha, seja de hardware ou software, interrompendo o funcionamento correto.	
Informações adicionais	
Gatilho	Imediato
Tempo de Recuperação Desejável	TMP = 1 hora NMD = 75% TMR = 2 horas
<p>TMP = Tempo Máximo de parada, até que a atividade reinicie.</p> <p>NMD = Nível Mínimo de desempenho da atividade após reinício.</p> <p>TMR = Tempo Máximo de retomada dos níveis normais de operação</p>	
Contingência	
Benner	<p>Avaliar/verificar o incidente com o equipamento de estação de trabalho problemático;</p> <p>Caso o problema for de hardware, substituir o periférico problemático;</p> <p>Caso o problema for de software, avaliar a situação e, se necessário, reinstalar o aplicativo problemático.</p>
RTO	2 horas
RPO	N/A

17. RESPONSABILIDADE DE ATIVAÇÃO E EXECUÇÃO

Abaixo são apresentados os papéis e as responsabilidades das pessoas quanto à tomada de decisão durante e após incidente. Estas pessoas são os responsáveis pela ativação dos planos, necessários para determinadas contingências ou no auxílio para execução de determinadas ações do plano.

Responsável	Nome	Departamento	Telefone
Gerente de TI	Cláudio Marcio	Datacenter	(47) 99151 8200
Gerente de TI	Jorge Espinhara	Infraestrutura de TI	(47) 99167-5111

18. CONTATO FORNECEDORES E PARCEIROS

Abaixo é apresenta a lista dos fornecedores e telefones para contato. Os fornecedores devem ser comunicados assim que identificada a indisponibilidade dos serviços prestados por eles.

Nome	Fornecedor	Serviços	Telefone 1	Demais contatos
Tulio	Oracle	Datacenter	(11) 99909 5183	
NOC 24x7	Multitask	Monitoramento Infra	(47) 99966-4815	Grupo do Teams/ Whatsapp
Alexandre	RGK	Suporte redes	(47) 99116-3154	
Juliano Cascaes	IP5	Suporte Servers	(47) 99119-0826	
NOC 24x7	Exímio	Monitoramento Banco de Dados	(47) 3053-7082	Grupo do Teams/ Whatsapp
MDR/SOC 24x7	Malwarebytes	EDR/Segurança	(11) 98282-3456	
Paulo	Callix	Telefonia VoIP	(11) 99607-3484	

19. PLANO DE AÇÃO PREVENTIVO, MONITORAMENTO E CONSCIENTIZAÇÃO

Para detectar possíveis falhas que possam comprometer os acessos, disponibilidade ou até mesmo negação de serviços, a operação é monitorada pelo NOC e SOC de forma contínua (24x7). Além do monitoramento, testes são realizados para validações da disponibilidade e integridade dos serviços.

- O recurso de backup tem por finalidade assegurar que as informações do sistema não sejam perdidas caso ocorra alguma falha de hardware ou de software.
- **Backup Banco de Dados:** Este backup é feito diariamente com recurso do Oracle RMAN com RPO de 60 minutos.
- **Backup Servidores:** Este backup é realizado semanalmente com cópia do disco/servidor virtual.
- **Monitoramento 24x7:** Realizado pela empresa Multitask 24x7 pelo portal monitoramento.benner.com.br além de ferramentas de MDR para realização do SOC. Todos os *threshold* de monitoramento são definidos específicos para cada operação ou cliente.
- **Conscientização:** Por meio de treinamentos contínuos, garantimos que todos os colaboradores, subcontratados e parceiros compreendam as práticas recomendadas, normas e políticas publicadas para saberem como agir diante de situações de risco. São apresentados conceitos de identificação de e-mails de phishing e engenharia social, proteção de credenciais, divulgação das políticas de segurança, com objetivo de capacitar colaboradores a atuarem como a primeira linha de defesa, a fim de reconhecer e reportar potenciais riscos ou incidentes de segurança.
- **Oracle Cloud Infrastructure – OCI:** O Ambiente Bennercloud está hospedado em território Nacional replicado em duas regiões (Oracle Brasil) com SLA de disponibilidade superior a 99,95% <https://www.oracle.com/br/cloud/sla/>
- **Servidores Virtuais e Rede:** A topologia e infraestrutura é 100% nativa Oracle OCI, com possibilidade de servidores replicados em múltiplas regiões, oferecendo mais disponibilidade e garantia de continuidade de negócio.

20. ELIGIBILIDADE E VALIDADE

Este documento aplica-se aos envolvidos no plano e substitui todos os outros anteriores. Entra em vigor a partir de 20.11.2023.

21. REGISTRO DE ALTERAÇÕES

Versão	Data	Etapa	Responsável
1.0	20/11/2023	Criação	Jorge Espinhara e Claudio Márcio

22. FORMALIZAÇÃO

REVISÃO		APROVAÇÃO	
Marcelo Murilo Silva – VP Saúde		Severino Benner - CEO	
23/11/2023		25/11/2023	