

**PLANO DE CONTINUIDADE DE NEGÓCIOS – INDÚSTRIA DE
BEBIDAS NÃO ALCÓOLICAS**

Desenvolvido por:

Igor Vinícius Moreira
Matheus de Andrade Vaz
Vitor Kiomassa Kina
Yan Moura Virginio

RA: 1680971711003
RA: 1680971711021
RA: 1680971711028
RA: 1680971711019

SÃO CAETANO DO SUL
30/05/2019

SUMÁRIO

CONTROLE DE VERSÃO DO PCN	3
INTRODUÇÃO	4
INFORMAÇÕES DA EMPRESA	4
PROCESSOS CRÍTICOS E SUAS PRINCIPAIS TAREFAS	4
TIPOS DE PLANOS	5
ANÁLISE DE RISCO	6
BUSINESS IMPACT ANALYSIS	7
REQUISITOS DE TEMPO PARA A RECUPERAÇÃO DOS NEGÓCIOS	7
REGRAS DE ACIONAMENTO	8
TREINAMENTO E PROGRAMA DE TESTES	8
REVISÃO E MANUTENÇÃO DO DOCUMENTO	9
RESPONSABILIDADES DE ACORDO COM O CARGO E TAREFA	10
RESPOSTA A INCIDENTES	11
RECUPERAÇÃO DE DESASTRES	12
SITES ALTERNATIVOS	17
COMUNICAÇÃO DO PCN	18
COMUNICAÇÃO EM ESTADO DE CONTINGÊNCIA	18
CONVENCIMENTO DA ALTA DIREÇÃO	18

CONTROLE DE VERSÃO DO PCN

Versão	Data	Nome	Ação	Conteúdo
1.0	17/05/2019	Igor Moreira Matheus Vaz Vitor Kina Yan Virginio	Elaboração	Primeira versão do documento
1.1	24/05/2019	Igor Moreira Matheus Vaz Vitor Kina Yan Virginio	Revisão	Revisão após a apresentação do PCN para a alta direção
1.2	30/05/2019	Igor Moreira Matheus Vaz Vitor Kina Yan Virginio	Revisão	Revisão para a entrega do documento à alta direção
		Gabriel Julio	Aprovação	Aprovação do documento pelo CIO Gabriel Julio

INTRODUÇÃO

Este plano de continuidade de negócio tem como intuito minimizar possíveis danos à organização em eventuais situações de estado de contingência, onde pode ocorrer interrupção na produção e processos críticos, riscos a segurança lógica dos ativos, catástrofes naturais ou não naturais, com ou sem o risco à vida.

Este PCN foca em manter o funcionamento de três processos críticos, essenciais para que a empresa atinja seus objetivos a longo prazo, são eles:

- Logística
- Marketing
- Controle de Qualidade

INFORMAÇÕES DA EMPRESA

Nome da Organização: Ambebe

Ramo da Organização: Refrigerantes e Energéticos

Localização: Sede – Curitiba, localizado na Cidade Industrial; Filiais – Rio de Janeiro e São Paulo

Quantidade de Colaboradores: Contratados – 500; Terceirizados – 500

PROCESSOS CRÍTICOS E SUAS PRINCIPAIS TAREFAS

Logística:

- Processo de Venda
- Processo de Roteirização
- Processo de Entrega
- Gestão de transportes
- Gestão da cadeia de suprimentos
- Relatórios de Mercadorias, criação de notas fiscais de entrada e saída

Marketing:

- Criação do Logotipo dos produtos
- Análise SWOT
- Merchandising
- Patrocínio de eventos
- Promoções sazonais
- Armazenamento do material de divulgação

Controle de Qualidade:

- Tratamento da água
- Verificação da qualidade do açúcar cristal
- Verificação da procedência dos concentrados e aditivos
- Manipulação da pureza do gás carbônico
- Filtragem do carvão ativo e da terra diatomácea
- Gestão da qualidade dos lotes de produtos fabricados

TIPOS DE PLANOS

Tipo de Plano	Equipe de tratativa
Plano de Continuidade de Negócios (PCN)	Equipe de Continuidade de Negócios
Plano de Continuidade Operacional (PCO)	Equipe de TI
Plano de Resposta a Incidentes (PRI)	CSIRT
Plano de Recuperação de Desastres (PRD)	Equipe de Recuperação de Desastres
Plano de Emergência Ocupacional (PEO)	Comitê de Emergência
Plano de Administração de Crises (PAC)	Comitê de Crises

ANÁLISE DE RISCO

Processo	Ativo	Vulnerabilidade	Ameaça	Riscos
Logística	Servidor de geração de notas fiscais	Falta de atualização da automação	Mal funcionamento da automação	Indisponibilidade para geração de notas fiscais
Marketing	Backup dos comerciais e identidade visual da empresa	Falta de processo de manuseio do backup	Manuseio incorreto do backup	Perda do backup das campanhas e identidade visual da empresa
Controle de qualidade	Servidor de Banco de dados	Privilégios excessivos ou esquecidos	Intervenção de um funcionário não autorizado ou inexperiente	Perda dos dados de um lote, coletados da produção do produto

Processo: Logística

Impacto: Alto

Controle preventivo: Atualização constante das aplicações usadas no servidor de geração de notas, implementações de serviços de contingência caso a automação principal falhe, treinamentos adequados aos funcionários para diminuição das falhas humanas e para mitigar o risco de falhas.

O processo de logística é um processo muito crítico para o segmento de bebidas não alcoólicas, pois se o sistema de notas fiscais não funcionar não será possível liberar os caminhões para que possa levar a mercadoria até o cliente que comprou e também não poderá deixar que o fornecedor descarregue no depósito também, o que pode trazer uma má relação com os parceiros da empresa.

Atividades: Criação de notas fiscais de entrada e saída, relatórios de mercadorias

Processo: Marketing

Impacto: Médio

Controle preventivo: criação de documento definindo um manuseio correto do backup de acordo com a norma ISO 27001.

O marketing tem um impacto médio na empresa, mesmo que a propaganda na empresa não sendo feita de forma correta afete nas vendas, a empresa continuará conseguindo vender, porém sendo necessária a criação de novos comerciais e propagandas onde acarretará um pequeno prejuízo financeiro.

Atividades: Armazenamento dos comerciais para divulgação

Processo: Controle de qualidadeImpacto: Alto

Controle preventivo: Política para exclusão do usuário no AD caso seja desligado da empresa, auditoria constante dos privilégios de usuários na rede, monitoramento contra um acesso não autorizado.

O controle de qualidade tem um impacto muito grande para empresa, perder os dados de um lote ou todas as informações sobre o seu produto significa que a empresa não tem controle sobre os seus produtos, podendo vender um lote que saiu estragado por exemplo, onde poderia causar uma baixa de reputação no mercado.

Atividades: Dados de qualidade de um lote, dados dos produtos fabricados.

BUSINESS IMPACT ANALYSIS

Questões qualitativas - escala de impacto: 1 - Impacto baixo, 2 - Impacto aceitável, 3 - Impacto alto, 4 - Impacto catastrófico	2 horas	4 horas	8 horas	24 horas	48 horas	1 semana
1) Como seus clientes reagirão a uma interrupção?	1	1	2	2	2	3
2) Qual será o impacto para outras atividades da organização?	1	2	2	3	3	4
3) Como a interrupção irá influenciar a perda de reputação?	1	1	2	2	3	3
4) O quão difícil será recuperar o trabalho perdido?	1	1	2	3	3	4
Questões quantitativas - definido em R\$						
5) Qual o custo das penalidades legais e contratuais?	0	0	0	30000	60000	210000
6) Qual serão os custos com reparos?	0	3000	6000	18000	36000	126000
7) Quanto de receita será perdida?	6000	12000	24000	72000	144000	504000

REQUISITOS DE TEMPO PARA A RECUPERAÇÃO DOS NEGÓCIOS

Tolerância Máxima de Inatividade	
MTD	48 Horas
Objetivo de Tempo para Recuperação	
RTO	8 Horas
Tempo de Trabalho para Recuperação	
WRT	24 Horas

REGRAS DE ACIONAMENTO

Evento	Plano acionado	Tratativa
Sistema de NFs não gera as notas de forma automatizada	Plano de Continuidade Operacional	Equipe de TI
Infecção por Malware nos servidores de armazenamento de arquivos da empresa	Plano de Resposta a Incidentes	CSIRT
Enchente no local da fabrica	Plano de Continuidade de Negócios; Plano de Administração de Crises; Plano de Emergência Ocupacional; Plano de Continuidade Operacional; Plano de Recuperação de Desastres	Equipe de Continuidade de Negócios; Comitê de Crises; Comitê de Emergência; Equipe de TI; Equipe de Recuperação de Desastres

TREINAMENTO E PROGRAMA DE TESTES

O treinamento deverá ser realizado com todos colaboradores, terceiros e prestadores de serviço que fazem parte do escopo do PCN. O treinamento será específico para cada colaborador com base nas atividades de cada um, incluirá prática (simulações) e teórica (apostila e testes), terá periodicidade de 6 em 6 meses e será realizado testes na semana seguinte ao treinamento para que se fixe os ensinamentos e para que seja realizada uma resposta bem articulada e rápida no caso de um incidente. Se houver alguma alteração impactante no PCN deverá ser realizado o treinamento e aplicação de testes com um tempo máximo de uma semana após a mudança no documento.

No programa de testes serão tratados:

- Simulações: Testes dos principais pontos de um procedimento para validação parcial de um plano.
- Testes de Mesa: Avaliar, através de check-lists, as ações descritas nos procedimentos, com o intuito de validar o conteúdo de um plano.
- Teste de atividades Críticas: Efetuar procedimentos de operações críticas em ambiente controlado para validação.

- Processo de Walkthrough: Conferir todos os passos descritos de um plano
- Teste Completo: Testar todos os pontos de um procedimento para validar de forma integral um plano.

Os testes efetuados para cada plano contido no PCN irá depender da criticidade do plano e o custo que determinado teste irá gerar para ser efetuado em determinado plano.

Relação Tipos de Teste com Tipo de Plano	
Teste de Mesa; Walkthrough	Plano de Continuidade de Negócios (PCN)
Teste de atividades Críticas; Teste de Mesa; Walkthrough	Plano de Continuidade Operacional (PCO)
Teste de Mesa; Walkthrough	Plano de Resposta a Incidentes (PRI)
Teste Completo; Walkthrough	Plano de Recuperação de Desastres (PRD)
Simulação; Teste de Mesa; Walkthrough	Plano de Emergência Ocupacional (PEO)
Simulação	Plano de Administração de Crises (PAC)

REVISÃO E MANUTENÇÃO DO DOCUMENTO

A atualização dos documentos será realizada pela equipe de segurança da informação. Os documentos serão atualizados em um prazo de no mínimo 8 meses e no máximo de um ano, porém poderão sofrer alterações fora deste prazo caso ocorram mudanças em relação aos processos críticos e ativos, ou caso ocorram novas adições de relevância suficiente para o mesmo ser revisado.

RESPONSABILIDADES DE ACORDO COM O CARGO E TAREFA

Nome	Cargo	Empresa	Atividades	Contato
Gabriel Julio	CIO	Ambebe	Direção da elaboração do projeto, aprovação de alterações.	gabrieljulio@ambebe.com.br (41)94587-5623
Vitor Kina	Analista de segurança da informação (e CSIRT)	Ambebe	Elaboração do projeto, realizar mudanças, análise dos processos.	vitorkina@ambebe.com.br (41)98465-2234
Marcos Siqueira	Patrocinador	Sevenarmy	Análise financeira, verificar viabilidade do projeto e sugerir alterações.	mgsiqueira@sna.com (11)97564-5624
Matheus Vaz	Diretor executivo	Ambebe	Elaboração do projeto, análise financeira interna, verificar viabilidade e sugerir alterações.	matheusvaz@ambebe.com (41)4543-4645
Yan Virginio	Gerente da linha de produção	Ambebe	Elaboração do projeto, verificar conformidade dos processos descritos de acordo com as atividades reais.	yanvirginio@ambebe.com.br (41)97845-7854
Igor Moreira	Gerente de RH	Ambebe	Elaboração do projeto, divulgação e treinamento.	igormoreira@ambebe.com.br (41)96457-7291
Ricardo Cruz	Gerente de Marketing	Ambebe	Realiza uma análise técnica, e participa da elaboração de alguns aspectos do documento.	ricardocruz@ambebe.com.br (41)98783-4685

RESPOSTA A INCIDENTES

Processo: Controle de qualidade

Ameaça: Intervenção de um funcionário não autorizado ou inexperiente

Ativo: Servidor de banco de dados

Resposta inicial: Documento 1.2. Responsável: CSIRT

Identificação: Para identificar essa ameaça é necessário fazer uma auditoria dos usuários que estão utilizando o servidor de banco de dados.

Primeiramente será necessário saber os usuários que realmente podem ter acesso ao servidor de banco de dados.

Após isso será necessário verificar as logs dos usuários que acessaram o servidor e comparar com a lista dos usuários que são autorizados.

Caso tenha algum funcionário não autorizado o acesso deve ser excluído imediatamente e o seu gestor deve ser acionado para possível advertência ou suspensão.

Verificar se houve alguma alteração feita por esse usuário no banco de dados caso sim, a ameaça foi concretizada e será necessário uma contenção da mesma.

Contenção: Caso o usuário não autorizado tenha feito alguma alteração será necessário recuperar o backup daquele banco de dados, pois pode ter sido perdido alguma informação muito importante para a organização.

Recuperar backup dos lotes e fazer auditoria para saber se existiu a perda de alguma informação.

Prevenção: Para evitar uma ameaça como essa, deve ser feito uma auditoria constante dos acessos e privilégios dos usuários da empresa e deve estar definido na política um provisionamento de acesso conforme controle 9.2.2 da ISO 27001 de segurança da informação.

RECUPERAÇÃO DE DESASTRES

Ativo: Servidores

Evento: Enchente no local da fábrica

Este Plano de Recuperação de Desastres (PRD) tem informações que descrevem os procedimentos a serem realizados caso ocorra enchente no local de fábrica e afete os servidores.

Escopo: O PRD da Ambebe tem como escopo todas as divisões da organização, seus departamentos e às pessoas que fazem parte do quadro de funcionários.

Planos e responsáveis: No caso de ocorrer esse desastre, os seguintes planos serão acionados: PCN; PAC; PEO; PCO; PRD. As equipes responsáveis por cada plano irão realizar um esforço conjunto para restabelecer a funcionalidade normal dos processos críticos.

As equipes de cada plano são:

- Equipe de Continuidade de Negócios (PCN)
- Comitê de Crises (PAC)
- Comitê de Emergência (PEO)
- Equipe de TI (PCO)
- Equipe de Recuperação de Desastres (PRD)

Equipe de continuidade de negócios deverá ser acionada primeiramente, desta forma os responsáveis pelo PCN ativarão os outros planos.

Contatos: Equipe de Continuidade de Negócios

Nome	Cargo	Telefone	E-mail
Jorge Palhos	Diretor de SI	(41) 94587-5623	jorge@ambebe.com.br
Eric Kun	Gerente de SI	(41) 3234-8413	eric@ambebe.com.br

A equipe de PCN acionará o comitê de crises e o comitê de emergência, este último verificará os procedimentos a serem seguidos e decisões a serem tomadas em situações de emergência.

Contatos: Comitê de Emergência

Nome	Cargo	Telefone	E-mail
Gustavo Novaes	Diretor Administrativo	(41) 5348-4245	gustavo@ambebe.com.br
Renato Filho	Gerente RH	(41) 5724-5350	renato@ambebe.com.br

O comitê de emergência acionará a equipe de TI, declarado o estado de contingência a equipe de TI acionará a equipe de recuperação de desastre e trabalhará em conjunto com ela para a retomada dos sistemas, ativos e processos críticos de TI.

Contatos: Equipe de TI

Nome	Cargo	Telefone	E-mail
Marcelo	Gerente de operacional	(41) 6452-9097	marcelo@ambebe.com.br
Alessandro	Gerente de sistemas	(41) 9794-0031	alessandro@ambebe.com.br

Equipe de TI aciona a equipe de recuperação de desastres, esta que fará o acionamento dos sistemas e restauração do backup do BD no hot site, quando o hot site estiver ativo e funcional, esta equipe trabalhará em conjunto com a equipe de TI para voltar à normalização da produção nos ativos e processos de TI no site original.

Contatos: Equipe de Recuperação de Desastres

Nome	Cargo	Telefone	E-mail
Ronaldo Alcântara	Administrador de Database	(41) 4255-0051	ronaldo@ambebe.com.br
Marcos Barros	Responsável pelos backups	(41) 4226-0825	marcos@ambebe.com.br

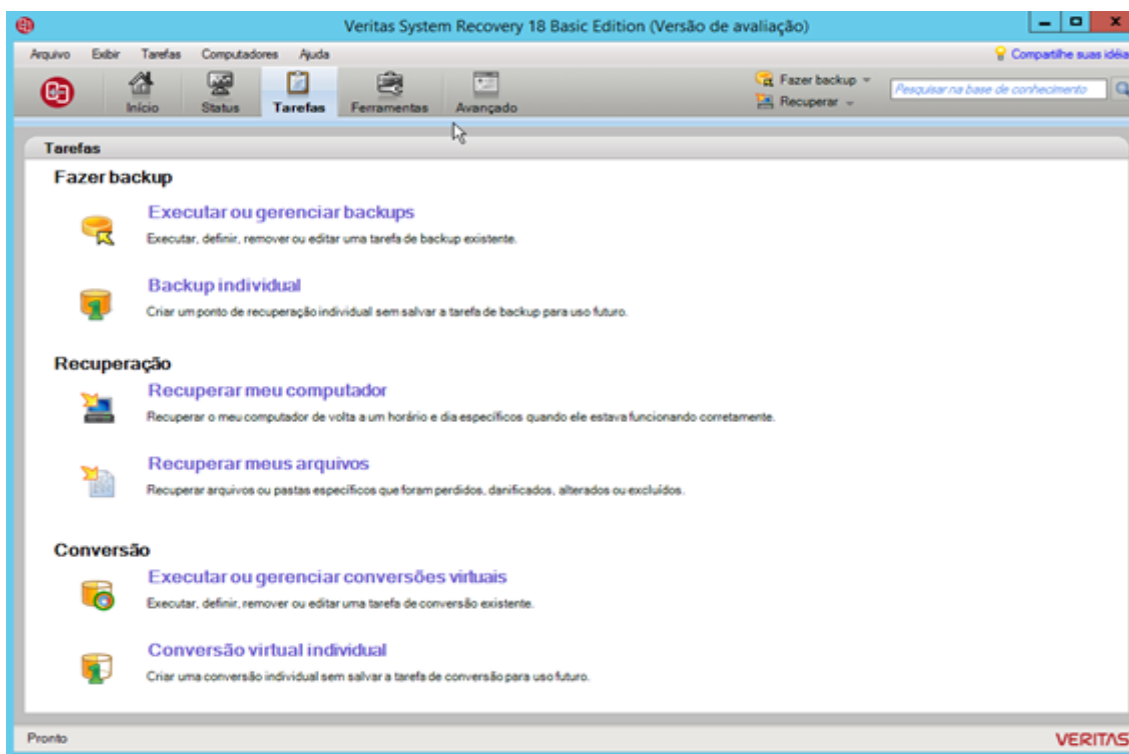
Comunicação

Será acionado o Comitê de Crises pela equipe de continuidade de negócios, o comitê que supervisionará todo o processo de recuperação e comunicará à imprensa sobre o andamento desta crise a fim de minimizar prejuízos à imagem da empresa.

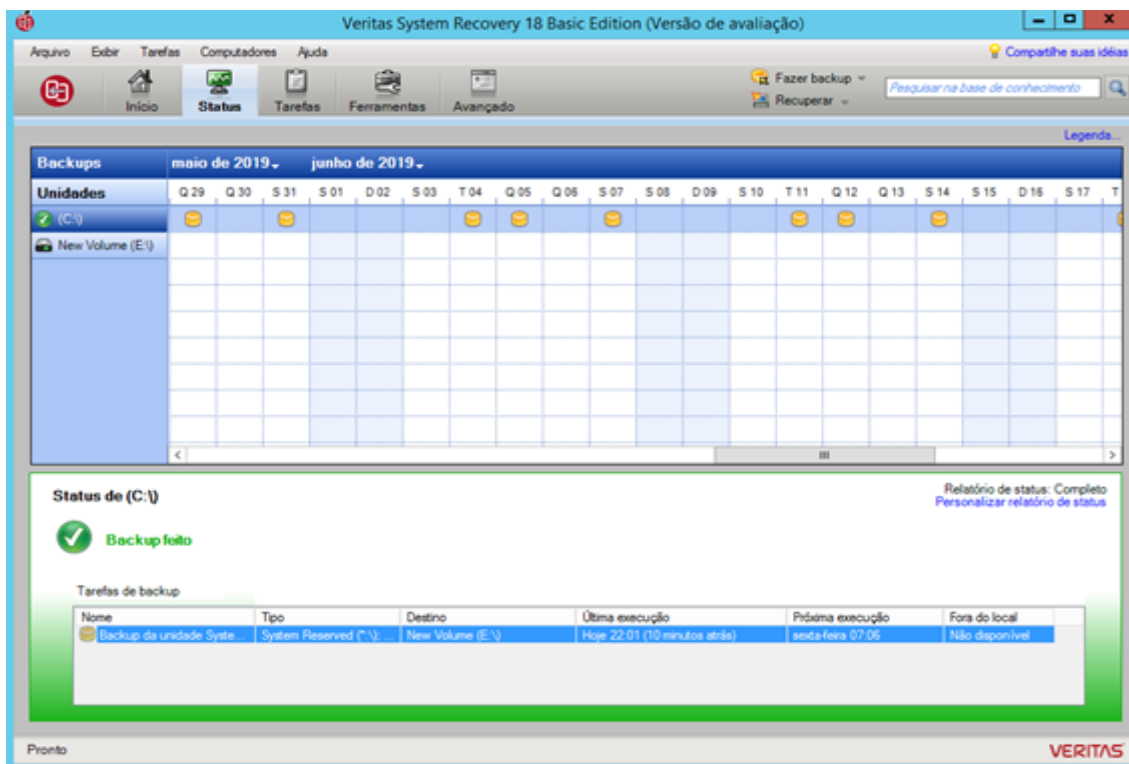
Recuperação dos sistemas

Será realizado backup dos principais processos de negócios da Ambebe, o sistema usado para backup e recuperação dos sistemas, dados e aplicativos será Veritas System Recovery 18 e os responsáveis serão a equipe de TI e equipe de recuperação de desastres. Após o desastre será acionado a equipe de recuperação de desastres que será responsável em acionar o site alternativo e pela restauração dos backups dos sistemas, dados e aplicativos da Ambebe. Segue abaixo imagens para realização do backup e restauração.

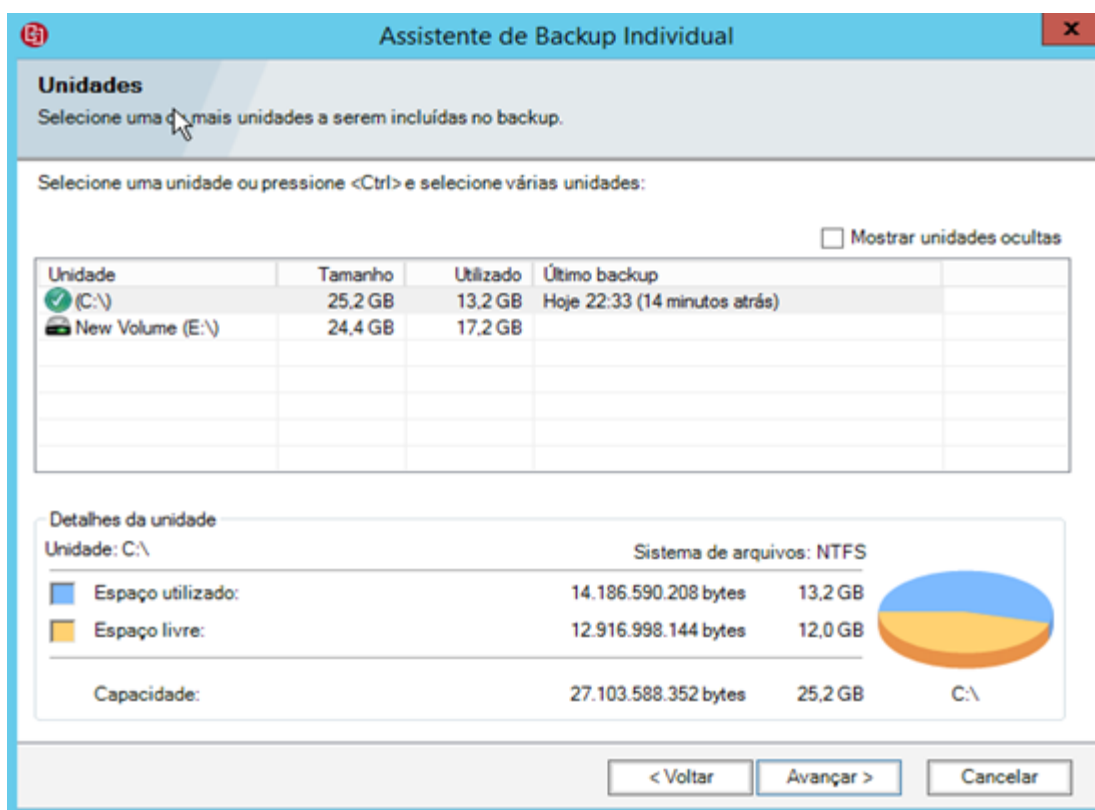
1. Tela de criação de backup, recuperação e conversão.



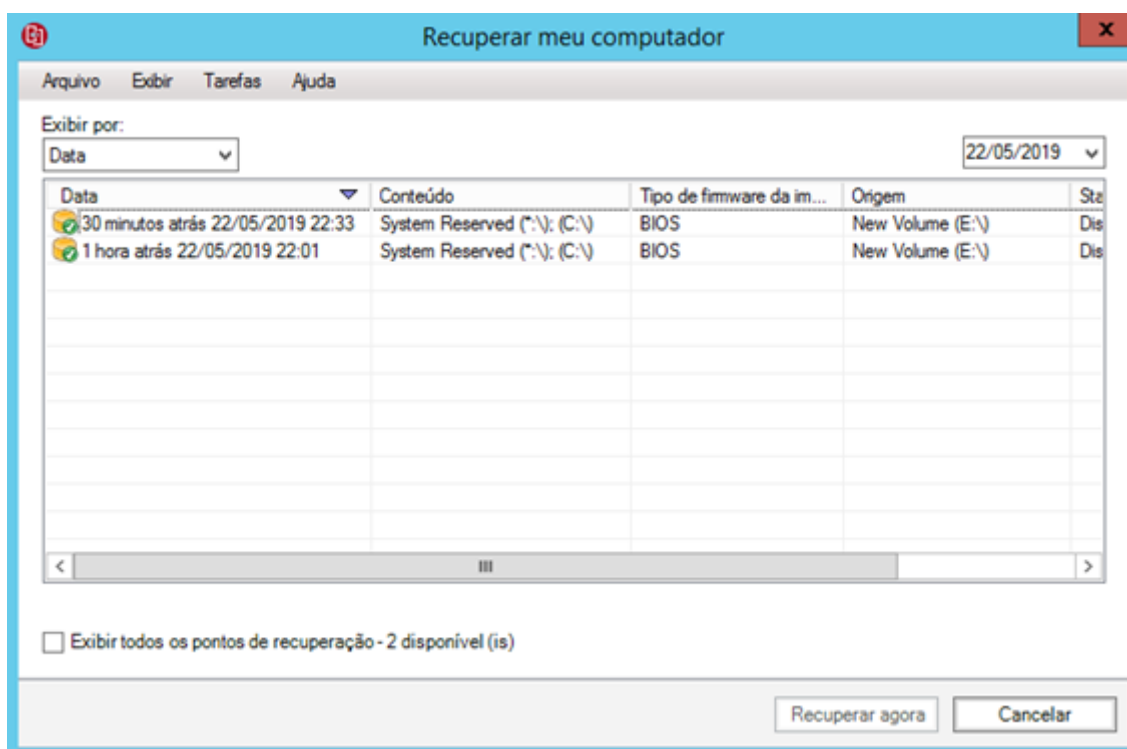
2. Tela de agendamento de backup



3. Tela para realização do backup



4. Tela para recuperação



SITES ALTERNATIVOS

A empresa Ambebe terá como site alternativo o Hot Site, pois é necessário ter um site que tenha uma recuperação imediata e tenha suporte à infraestrutura de servidores, cabeamento e telecomunicação.

Localização e descrição do site

O site é localizado no DataCenter da ITOne em Campo Belo/SP, em caso de ativação do site a equipe de recuperação de desastres entraram em contato com a ITOne.

O tempo estimado da operação lógica é de uma janela de meia a uma hora, porque não é necessário preparar toda a infraestrutura antecipadamente sendo assim somente necessário efetuar a restauração dos backups dos bancos de dados. Os dados de aplicação, dados de configuração e dados de segurança são replicados periodicamente para o site para que caso ocorra o incidente o site alternativo já contenha os dados tornando a recuperação mais rápida e eficiente.

COMUNICAÇÃO DO PCN

Responsável pela divulgação: Gerentes de cada filial da empresa Ambebe.

O plano estará armazenado como documento PDF no seguinte diretório de rede \\192.168.15.150\informativos\documentos\PCN e também um material impresso como forma de arquivo, esse material estará armazenado no RH.

Os colaboradores terão acesso a esse diretório de acordo com seu login, todos receberão o link do diretório através do seu endereço de e-mail e também será publicado nos murais da empresa, porém dependendo do tipo de usuário não terá acesso a todo o documento mas sim a parte que lhe convém (respeitando o nível hierárquico).

Arquivo estará armazenado na rede interna da empresa sendo protegido pelo backup com todos os outros arquivos de diretórios de rede.

COMUNICAÇÃO EM ESTADO DE CONTINGÊNCIA

Caso ocorra um incidente e seja necessário entrar no estágio de contingência a comunicação com os setores é algo crucial. A equipe responsável por ter comutado um sistema da empresa para contingência deve avisar ao líder de cada área, que avisará aos funcionários. Isso é de extrema importância para que todas as partes envolvidas estejam bem informadas e para passar toda a tratativa e os esforços necessários para o restabelecimento dos serviços inativos.

CONVENCIMENTO DA ALTA DIREÇÃO

Por ser de extrema importância para uma empresa, pois garante que a mesma consiga se recuperar em caso de falha, o convencimento da alta direção em efetuar a aquisição do plano irá se focar mais na parte de custo, tentando utilizar com o maior custo benefício possível o valor que seria investido para garantir o bom andamento do documento. Para isso, utilizaremos números estatísticos e situações hipotéticas, exemplificando as situações onde o PCN será utilizado.