Política e Plano de Continuidade de Negócios

Uso Interno

Junho 2024

azimut

CONTEÚDO

1. Introdução

A AZIMUT BRASIL (“AZBR”), alinhada com as diretrizes do Grupo Azimut, neste documento estabelece sua Política e Plano de Continuidade de Negócios (PCN).

2. Público Alvo

As regras contidas nesta Política aplicam-se às pessoas vinculadas.

Definimos como Pessoas Vinculadas:

- profissionais com vínculo CLT e estagiários;
- administradores, empregados e demais prepostos que desempenhem atividades na AZBR ou em qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;
- assessores de investimento (AI) que prestem serviços ao intermediário;
- profissionais que mantenham contrato de prestação de serviços com a AZBR ou com qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;
- pessoas naturais que sejam, direta ou indiretamente, participantes do quadro societário da AZBR ou de qualquer empresa pertencente ao grupo econômico da AZ Brasile Holding Ltda;

O descumprimento de quaisquer das diretrizes estabelecidas por esta Política será considerado infração grave, sujeitando seu autor às sanções cabíveis, nos termos da legislação aplicável.

3. Objetivo

Esse documento visa descrever a estratégia de continuidade de negócios da AZBR que tenham sido interrompidos por eventos que impeçam a continuidade de suas atividades, ainda que temporariamente. Em razão do caráter confidencial que a atividade da AZBR está sujeita, esse documento irá descrever de forma sucinta os processos de contingência.

4. Responsabilidades

4.1 Diretorias e Gerências

- Deverão acompanhar e apoiar as áreas sob sua responsabilidade, certificando-se de que estejam em conformidade com a regulamentação e normas aplicáveis aos negócios da instituição; bem como respeitar as políticas, manuais e procedimentos internos estabelecidos e implementados na AZBR.
- Acompanhar sua equipe e promover orientação no cumprimento desta política.

4.2 Área deTecnologia da Informação (TI)

- Manter esta Política e outros Normativos Corporativos relacionados à área atualizados;

- Assegurar o comprimento das diretrizes estabelecidas;
- Elaborar, manter e testar periodicamente o plano de continuidade do negócio que assegurem a proteção e integridade física dos dados, dos ambientes e equipamentos de processamento e que permitam, em situações de emergência, reação imediata e rápida recuperação das informações, sem prejuízo das rotinas operacionais essenciais à condução dos negócios da organização;
- Revisar periodicamente suas instalações, a fim de assegurar o funcionamento dos sistemas de segurança do local de processamento de dados, tais como sistema de acesso, controles de temperatura e umidade ambiental, extintores etc.;
- Divulgar os programas de proteção e planos de contingência, de forma a assegurar que todos os colaboradores da organização saibam quais as suas funções e responsabilidades em caso de contingência ou desastre;
- Revisar o Plano de Contingência, anualmente ou sempre que necessário.

4.3 Compliance

- Informar mudanças regulatórias que, de alguma forma, possam impactar esta Política.

4.4 Auditoria Interna

- Revisar e avaliar a eficiência quanto à implementação e aos controles da instituição.

4.5 Pessoas Vinculadas

- Conhecer e cumprir as Políticas, Manuais e procedimentos adotados pela instituição.

5. Diretrizes

- Processos, sistemas e dispositivos redundantes estão disponíveis para garantir a continuidade da operação, ou alternativamente um downtime mínimo da operação dos processos críticos de negócio;
- São tratados, minimamente, os seguintes aspectos:
  - Comprometimento da segurança da infraestrutura de tecnologia, no todo ou em parte, de forma a afetar a continuidade da operação dos processos críticos de negócio;
  - Acidentes ou incidentes nos aspectos físico e lógico;
  - Indisponibilidade da infraestrutura de tecnologia ou de ativos de suporte aos processos críticos de negócio;
  - Fraudes.
- A execução do plano prevê a minimização do downtime pela execução dos processos e uso dos dispositivos de contingência, a avaliação das causas, providências corretivas e retorno ao processo normal de produção, nesta ordem;
- Sistemas considerados críticos somente entram em produção após testes e aprovação do seu processo de contingenciamento.

6. Elaboração do Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais à AZBR sejam devidamente identificados e preservados após a ocorrência de uma contingência.

O Plano de Continuidade de Negócios da AZBR está baseado nas recomendações do DRI (Disaster Recovery Institute International) e DRJ (Disaster Recovery Journal).

Os itens que devem ser observados em um plano de continuidade de negócios de acordo com a DRI encontram-se abaixo listados:

- Projeto Start-up e Administração;
- Avaliação e controle dos riscos;
- Análise de impacto dos negócios;
- Orientação estratégica do desenvolvimento da continuidade;
- Respostas e operações em casos de emergência;
- Consciência e Programas de treinamento de implementação;
- Manter e dar suporte ao Plano de continuidade de negócios;
- Parceria com entidades privadas.

A gestão e organização do projeto de contingência está sob a gestão e supervisão do Diretor responsável pela área de TI.

6.1 Projeto Start-up e Administração

É estabelecido o escopo (necessidades) para o desenvolvimento do plano de continuidade de negócios. Isso inclui questões de suporte para realização, organização e gestão do projeto.

6.2 Avaliação e Controle de riscos

Define os cenários e os eventos prováveis que fazem parte do cenário corporativo e que podem afetar a AZBR e suas instalações, seja nas hipóteses de interrupções ou de desastres. Os eventos prováveis para a operação do plano de continuidade de negócios seriam: acesso proibido ao edifício em razão de acidentes, desastre com o edifício, mau funcionamento de hardware ou software, ou por razões de caso fortuito ou força maior (desastre natural).

6.3 Análise de impacto dos negócios

Identifica e avalia as interrupções e os cenários de desastres que podem afetar a AZBR, assim como as técnicas para quantificar e qualificar esses impactos. Isso define o principal nível dos processos de orientação do negócio e a prioridade na sua recuperação, de modo que o tempo ideal de recuperação seja encontrado.

O projeto de contingência consiste na acomodação de usuários, estrategicamente escolhidos pelos membros da diretoria da AZBR, onde o ambiente será acessado via VPN, no regime de home office. Dentre esses principais usuários, temos o responsável pela área de backoffice e de gestão. O contato das pessoas-chave para a restauração das atividades da empresa é realizado por meio de telefone e e-mail.

A AZBR também possui as rotinas de backup realizadas diária, semanal e mensalmente, que são armazenadas na plataforma em nuvem chamada Azure. Neste procedimento é considerado o file server completo, ou seja, de todas as pastas na rede e dos bancos de dados dos servidores, e as informações são salvas em instalações diferentes do local de processamento principal.

No que diz respeito aos prazos estipulados para arquivamento dos backups, estes serão mantidos nos prazos: backup diário por 03 meses, mensal por 12 meses e o anual por 05 anos.

Os backups são testados diariamente no próprio ambiente em que são realizados, do Azure. O acesso ocorre por meio de login e senha do usuário administrador em posse do responsável pela área de TI.

Demais testes são realizados periodicamente com a seguinte cobertura:

1) Teste de queda de energia
2) Teste de queda de telefonia
3) Teste de link primário
4) Testes de acesso remoto
5) Teste no firewall
6) Teste com link da RTM
7) Teste com cameras de circuito interno
8) Teste com servidores

Todas as deficiências deverão ser apresentadas, avaliadas por TI e reportadas para a diretoria. Em caso de situações de impacto e falhas encontradas durante os testes, estes serão avaliados por TI e as correções apresentadas aos membros da diretoria, que tomarão as decisões para a execução das providências de correção por parte da equipe de TI.

6.4 Orientação estratégico do desenvolvimento da continuidade

Define e orienta a eleição de estratégias operacionais alternativas para a recuperação dos processos e componentes do negócio no tempo desejado para recuperação, enquanto os processos corporativos críticos são mantidos em atividade.

Para cada evento ou situação de emergência, um plano de ação do projeto de contingência é detalhado. Caso haja a necessidade de migração dos processos críticos para o local de *backup*, este possui equipamentos adequados para a continuidade das operações da AZBR. Os dados do *backup* podem ser recuperados remotamente por meio de conexões dedicadas ou por unidades de armazenamento mantidas em locais seguros.

O acesso às conexões dedicadas e às unidades de armazenamento só podem ser acessados mediante utilização de login e senha do usuário administrador em posse, responsável pela área de TI.

6.5 Respostas e operações em casos de emergência

Desenvolve instrumentos de resposta e os procedimentos em caso de incidente ou eventos, incluindo criação e especificação de normas de gestão para execução das atividades operacionais fora do escritório central durante os períodos de crise.

O prazo máximo para a restauração e/ou disponibilização de infraestrutura para a execução das atividades primordiais/essenciais é de 5 horas. Em casos em que ocorra uma parada superior a este prazo estipulado, é acionado o plano de contingência.

Em casos de situação de crise (sem os serviços essenciais por mais de 5 horas) é de responsabilidade dos membros da Diretoria acionarem o Banco Central do Brasil de forma tempestiva, comunicando sobre o evento e o plano de ação em curso para a normalização.

6.6 Manutenção e suporte

Define um pré-plano e coordena as tarefas do plano de continuidade de negócios, avaliando os resultados obtidos. Apresenta a comparação entre os resultados obtidos e o ambiente corporativo convencional de trabalho, demonstrando as diferenças de forma clara.

A AZBR elaborou um plano de ação, onde estão descritos todos os processos necessários para a realização do plano de contingência, assim como as pessoas responsáveis pela coordenação e execução do plano de continuidade de negócios. Periodicamente, este plano é atualizado de acordo com as simulações realizadas e o surgimento de novos processos críticos da empresa.

6.7 Relações Públicas e Gerenciamento da Crise

Coordena, avalia e exercita mídias e documentos acessíveis durante situações de crise, assim como meios de comunicação para minimizar impactos traumáticos entre a AZBR, as pessoas vinculadas, clientes, fornecedores, investidores, parceiros e gestores.

Garante que todos os investidores sejam informados por meio de uma única fonte constantemente atualizada.

Em caso de remoção da empresa para o local de *backup*, todos os investidores serão informados através de e-mails que serão enviados do próprio local de *backup*.

6.8 Resultado

A análise de todos os pontos e informações dos itens acima levaram à elaboração de um plano de gerenciamento de contingências que possam eventualmente interromper o desenvolvimento das atividades da AZBR.

O plano de ação desenvolvido tem início tão logo identificado qualquer evento impeditivo do desenvolvimento de suas atividades, por meio de comunicado ao responsável pela área de TI.

Restaurados os sistemas, dados e servidor, são liberados os acessos a cada uma das pessoas-chave das áreas vitais para a continuidade das atividades da AZBR, a saber, responsáveis pela área de backoffice e de gestão.

7. Plano de Continuidade de Negócios

As ações da diretoria e do TI variam de acordo com impacto dos incidentes, podendo ser um simples acionamento de um backup de dados dos servidores até incidentes de maior magnitude que demandarão o acionamento do contingenciamento do local de trabalho, através, por exemplo, da liberação de acesso VPN a todos os colaboradores para que estes exerçam suas funções estando em suas residências ou em escritórios em diferentes localidades.

Portanto, o acionamento para continuidade de negócios será realizado pelos membros da diretoria em conjunto com a área de TI, sejam quais forem os eventos.

8. Disposições Gerais

Todas as pessoas vinculadas devem sentir-se envolvidas e responsáveis pelo aprimoramento dos Controles Internos de forma a mitigar riscos e na busca constante da eficiência e integridade no desempenho das atividades.

Todo o conteúdo descrito nesta política é de propriedade da AZBR, não devendo ser divulgado ou disponibilizado para quaisquer outras pessoas, firmas, entidades e/ou partes externas à empresa, salvo em casos previamente analisados e formalmente aprovados.

O seu descumprimento é passível de aplicação de medidas disciplinares, conforme previsto no Código de Ética e Conduta.

9. Informações de Controle

Vigência: 2 anos.

Versão: 04/2024

Atendimento a necessidades específicas:

( ) Sox
( ) Basiléia
(X) Outros: Políticas internas da AZBR
( ) Não Aplicável

Versão	Item alterado	Descrição resumida da alteração	Motivo	Data
1	-	-	Elaboração da Política	Abril 2016
2	Todos	Revisão geral do documento, visto que a primeira versão foi criada pela GESTORA e nesta versão a aplicação está sendo ampliada para AZBWM (GESTORA e DTVM). Ajuste da definição de pessoas vinculadas.	Revisão da Política	Março 2019
3	1 e 2	Atualização da normativa, de dados societários	Revisão da Política	Julho 2022
4	Todos	Revisão periódica prevista	Revisão da Política	Junho 2024

10. Responsáveis pelo Documento e Aprovações

Atividade	Nome	Nome da área	E-mail
Azimut Brasil WM	Wilson Barcellos	CEO	wilson.barcellos@azimutwealth.com.br

Azimut Brasil DTVM	Guilherme Doneux	Produtos	guilherme.doneux@azimutwealth.com.br
Azimut Brasil DTVM	Elisa de Plácido	Compliance / Risco	elisa.placido@azimutwealth.com.br
Azimut Brasil WM	Marcelo Sepulveda	Operações / TI	marcelo.sepulveda@azimutwealth.com.br
Azimut Brasil WM	Leonardo Monoli	Gestão	leonardo.monoli@azimutwealth.com.br