PLANO DE CONTINUIDADE DE NEGÓCIOS

CONTROLE DE APROVAÇÃO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Ana Carolina Almeida Analista de Sistemas	**Saul Barroso** Diretora de Controles Internos, Riscos e Compliance **Eli Tassim** Diretor Controller	**Saul Barroso** Diretora de Controles Internos, Riscos e Compliance **Eli Tassim** Diretor Controller

1 INTRODUÇÃO 4
2 ABRANGÊNCIA 4
3 ALÇADA DE APROVAÇÃO 4
4 RESUMO DA VERSÃO 4
5 VIGÊNCIA E ATUALIZAÇÕES 4
6 CONTINGÊNCIAS 5
7 EQUIPE 5
8 SITES DE CONTINGÊNCIA 6
9 CONTIGÊNCIAS DE INFRAESTRUTURA FÍSICAS 6
9.1 SITUAÇÕES DE CONTINGÊNCIA PREVISTAS: 7
9.1.1 Desastres e Catástrofes Naturais ou não Abrangência: 7
9.1.2 Danos físicos relevantes a instalações ou equipamentos críticos intencionais ou não 7
9.1.3 Falhas no fornecimento de energia elétrica 8
10 CONTINGÊNCIAS DE PESSOAL 8
10.1 SITUAÇÕES DE CONTINGÊNCIAS PREVISTAS 9
10.1.1 Ausência de colaboradores Chave por greves 9
10.1.2 Ausência de Colaboradores Chave por Licença Médica ou Maternidade / Paternidade 10
11 CONTINGÊNCIAS DE INFRAESTRUTURAS TECNOLÓGICAS ESTRUTURA DISPONIBILIZADA 11
11.1 SITUAÇÕES DE CONTINGÊNCIAS PREVISTAS 12
11.1.1 Falha em servidor de arquivos e banco de dados 12
11.1.2 Falha no Banco de Dados SQL 12
11.1.3 Falha na Rede - Switch 13
11.1.4 Falha no Sistema de Refrigeração da Sala dos Servidores/Equipamentos Data Center 14
12 CONTINGÊNCIAS DE SERVIÇOS EXTERNOS 14
12.1 SITUAÇÕES DE CONTINGÊNCIA PREVISTAS 14
12.1.1 Manutenção de posições de clientes 14
12.1.2 Liquidação de operações com clientes 15
12.1.3 Serviços de administração de fundos 15

12.1.4 Informações cadastrais 16

12.1.5 Gerenciamento de documentos 16

ANEXO 1 – PLANO DE CONTATO 16

ANEXO 2- CRONOGRAMA DE TESTES 17

ANEXO 3- DENIFINIÇÃO DE PRIORIDADES 17

1 INTRODUÇÃO

O Plano de Contingência e de Continuidade de Negócios pode ser entendido como o conjunto de medidas preventivas e procedimentos de recuperação, no caso de qualquer interrupção de negócios. Estas medidas vão muito além da simples adoção de um plano de seguro e, devem garantir a capacidade da AZUMI DTVM ("AZUMI") em operar em bases contínuas. Para tanto, esse plano deve assegurar que todos os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados.
Este Plano de Contingência e de Continuidade de Negócios tem por objetivo atender os cumprimentos legais e regulatórios e em atenção ao disposto na Resolução Bacen nº 4.893, de 26 de fevereiro de 2021 e em conformidade com os termos Códigos aplicáveis da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA ("ANBIMA")

2 ABRANGÊNCIA

O público-alvo desta Política são todos diretores e colaboradores da AZUMI, bem como estagiários e os prestadores de serviços.

3 ALÇADA DE APROVAÇÃO

TI – Elaboração deste manual

Diretora de Compliance e Diretor Controller – Revisão deste manual

Diretora de Compliance e Diretor Controller – Aprovação deste manual

4 RESUMO DA VERSÃO

09/02/2024 – Versão Original

19/02/2021 – Versão Revisada

20/07/2021 – Versão Revisada

18/07/2022 – Versão Revisada

15/08/2024 – Versão Revisada

16/07/2025 – Versão Revisada

5 VIGÊNCIA E ATUALIZAÇÕES

As diretrizes contidas neste Plano entram em vigor na data de sua publicação e permanecem vigentes por prazo indeterminado, devendo ser revisada anualmente ou em prazo inferior, sempre que solicitado pelo órgão regulador, em casos de alteração de legislação aplicável, ou ainda, se houver alteração no modelo de negócios, previamente validado pelo Compliance e Controles Internos e Comitê de Contingência.

6 CONTINGÊNCIAS

O Plano de Contingência e de Continuidade de Negócios envolve basicamente quatro grupos:

Contingências de Infraestrutura físicas: Assim compreendidas as situações de catástrofes naturais ou não, tais como inundações, incêndios, desabamentos etc. que impeçam o acesso e/ou utilização das instalações da AZUMI, como também danos físicos relevantes a instalações e/ou equipamentos, intencionais ou não e ainda falhas no fornecimento de energia elétrica.

Contingências de Pessoal: Aquelas onde os associados-chave não estão presentes por motivos de greves, doença, licenças etc.

Contingências de Infraestruturas tecnológicas: Compreendidas as situações de inacessibilidade, falha ou perda de quaisquer recursos de TI, tais como hardware, software, Telecom, rede e segurança.
Contingências de serviços externos: Compreendidas as situações de não prestação de serviço contratado considerado crítico / essencial aos processos da AZUMI.

O presente Plano de Contingência e de Continuidade de Negócios é de uso da AZUMI, sendo sua manutenção e atualização de responsabilidade do COMITÊ de CONTINGÊNCIA, a fim de mantê-lo consistente com as operações e estratégias correntes. Além disso, este plano deve ser testado periodicamente para assegurar que a AZUMI possa executá-lo num evento de descontinuidade dos negócios.
Este manual está disponível na intranet com acesso restrito a esse grupo, por conter informações estratégicas da AZUMI.

7 EQUIPE

O Plano de Contingência e de Continuidade de Negócios deve ser de pleno conhecimento do COMITÊ de CONTINGÊNCIA, cuja responsabilidade é gerenciar todo o da AZUMI em quaisquer das situações de contingência previstas nesse manual. Esse grupo é soberano em qualquer decisão em situações de contingência e é formado pelo responsável da área de TI Infra, pelo responsável da área de TI Desenvolvimento; pelo diretor Tecnologia, pelo diretor responsável por Risco Operacional e pelo diretor da Administração e tem a responsabilidade de eleger seus substitutos em caso de suas ausências.
Cabe ao COMITÊ de CONTINGÊNCIA:

(i) Identificar e analisar impactos nos negócios e perdas potenciais;
(ii) Garantir a continuidade dos negócios, operações e serviços;
(iii) Priorizar os processos críticos definidos corporativamente, incluindo todas as atividades da linha de frente às áreas de suporte;

(iv) Estabelecer detalhadamente todas as atividades, procedimentos, responsabilidades e necessidades de recursos no momento de uma eventual interrupção no Plano de Contingência e Continuidade de Negócios;

(v) Garantir que as informações sobre o plano de contingência e de continuidade de negócios estejam sempre atualizadas e acessíveis (física e eletronicamente);

(vi) Informar novos funcionários sobre o plano existente na instituição e, incentivar a participação no treinamento do plano de contingência e de continuidade de negócios;

(vii) Definir responsabilidade de atuação para cada funcionário, na execução do plano de contingência e de continuidade de negócios;

(viii) Manter equipes treinadas nas suas respectivas responsabilidades para agilizarem o processo de recuperação e continuidade de qualquer negócio;

(ix) Analisar periodicamente a documentação existente para suportar a restauração do ambiente em situação de contingência;

(x) Manter uma lista de contatos atualizada, inclusive de principais fornecedores e clientes;

(xi) Testar as ações para restauração do ambiente;
(xii)Simular situações emergenciais;
(xiii) Preparar ações necessárias à recuperação do funcionamento regular da AZUMI.

8 SITES DE CONTINGÊNCIA

A AZUMI contratou o serviço de Cloud Link da empresa RTM SOLUÇÕES inscrita no CNPJ sob o nº 30.411.616/000116.

O Cloud Link fornece conectividade dedicada, segura e com redundância às principais nuvens públicas do mercado, utilizando infraestrutura própria e de alta disponibilidade. Com acesso via rede lan to lan, proporciona alta velocidade e baixa latência, sem a necessidade de passar pela internet

A AZUMI conta ainda com infraestrutura 100% em cloud, que permite o acesso remoto em home-office ou através de coworking, utilizando ferramentas como webmail, celulares com serviço de e-mail e acesso remoto à rede que permitem que os associados possam realizar tarefas fora do ambiente do escritório, utilizando conexão OpenVPN Connect segura.

9 CONTIGÊNCIAS DE INFRAESTRUTURA FÍSICAS

Implantar um ambiente de contingência de trabalho remoto seguro envolve várias etapas para garantir que os dados e as comunicações da empresa estejam protegidos e funcionais. Aqui estão alguns passos essenciais:

1. **Definir Políticas de Segurança:**
   - Estabeleça políticas claras para o uso de dispositivos pessoais e corporativos.
   - Defina regras para o acesso a dados sensíveis e uso de redes não seguras.
2. **Implementar VPN:**
   - Use uma VPN (Rede Privada Virtual) para criptografar o tráfego de dados entre os dispositivos dos funcionários e a rede corporativa. OpenVPN é uma boa opção para configurar uma VPN segura.
3. **Utilizar Autenticação Multifator (MFA):**
   - Adote a autenticação multifator para acessar sistemas corporativos, o que adiciona uma camada extra de segurança além da senha.
4. **Gerenciar Dispositivos e Acessos:**
   - Implemente um sistema de gerenciamento de dispositivos (MDM) para controlar e proteger os dispositivos dos funcionários.
   - Use ferramentas de gerenciamento de identidade e acesso (IAM) para garantir que apenas usuários autorizados possam acessar sistemas e dados.

5. **Educar os Funcionários:**
   - Ofereça treinamentos regulares sobre boas práticas de segurança, como identificar e evitar phishing e usar senhas fortes.
6. **Manter Software Atualizado:**
   - Assegure que todos os sistemas operacionais, aplicativos e antivírus estejam atualizados para proteger contra vulnerabilidades conhecidas.
7. **Monitorar e Responder a Incidentes:**
   - Implemente soluções de monitoramento de segurança para detectar atividades suspeitas e tenha um plano de resposta a incidentes em caso de violação de segurança.
8. **Realizar Avaliações de Segurança Regulares:**
   - Faça auditorias e avaliações de segurança periódicas para identificar e corrigir possíveis vulnerabilidades.

9.1 SITUAÇÕES DE CONTINGÊNCIA PREVISTAS:

9.1.1 Desastres e Catástrofes Naturais ou não Abrangência:

Compreendem as situações de incêndios, inundações, desabamentos que exijam a imediata saída das instalações AZUMI.

Contingências existentes:

Os colaboradores, caso não seja possível breve retorno às dependências da AZUMI, serão divididos em grupos e serão direcionados para trabalho remoto utilizando-se das mesmas ferramentas.

O COMITÊ de CONTINGÊNCIA deverá avaliar o tempo de retorno às instalações e, se necessário, dividirá o staff da AZUMI para atender a contingência acima detalhada, atentando que, deverão ser encaminhados minimamente os colaboradores chave descritos no item de CONTINGÊNCIA de PESSOAS – Aspectos Gerais.

Retorno à normalidade:

Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos colaboradores o retorno às instalações da AZUMI.

9.1.2 Danos físicos relevantes a instalações ou equipamentos críticos intencionais ou não

Compreendem as situações de danos a instalações ou equipamentos da AZUMI de tal forma que impeçam a utilização de suas dependências ou de algum equipamento relevante para suas atividades.

Contingências existentes:

Todos os equipamentos críticos possuem contrato de manutenção com o fabricante com “tempo de solução”, tempo esse que varia conforme a criticidade do equipamento em questão.
Os colaboradores, caso não seja possível breve retorno às dependências da AZUMI, serão divididos em grupos e serão encaminhados para trabalho em home-office ou coworking.

Procedimentos:

Responsável: COMITÊ de CONTINGÊNCIA

Ativação da contingência:

O COMITÊ de CONTINGÊNCIA avaliará o tempo de retorno às instalações ou de conserto / substituição de equipamentos e, se necessário, dividirá o staff da AZUMI no site de contingência acima detalhados e para residências e/ou escritórios alugados com acesso remoto através de um túnel vpn criptografado, cada funcionário terá um login e senha individual para conexão. Atentando deverão ser encaminhados minimamente os associados chave descritos o item de CONTINGÊNCIA de PESSOAS.

Retorno à normalidade:

Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos colaboradores o retorno às instalações da AZUMI.

9.1.3 Falhas no fornecimento de energia elétrica

Compreendem as situações de problemas no fornecimento de energia elétrica por parte das concessionárias de serviços públicos, por “apagões”, por falhas na rede elétrica das dependências internas do da AZUMI etc., que acarretem a interrupção das atividades da AZUMI.

Contingências existentes:

Geradores no condomínio da sede da AZUMI, e equipamentos de nobreak nas dependências do escritório.

Procedimentos:

Responsável: Diretor de Tecnologia e TI Infra

Ativação da contingência

No caso de falha no fornecimento de energia elétrica o Gerador é acionado automaticamente após 20 segundos em caso de necessidade o nobreak será acionado automaticamente. A equipe de TI INFRA verificará imediatamente a extensão da falha no serviço e gerenciará a autonomia do gerador.

Caso ocorra falha no gerador e a energia seja mantida apenas pelo nobreak, como solução alternativa, a equipe de TI INFRA juntamente com o COMITÊ de CONTINGÊNCIA poderá determinar a necessidade de uso da contingência, podendo deslocar os colaboradores para trabalho em home-office ou coworking, utilizando-se com acesso remoto à rede da AZUMI.

Retorno à normalidade:

Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos colaboradores o retorno às instalações da AZUMI.

10 CONTINGÊNCIAS DE PESSOAL

Política de “substitutos” para funções chave

Para cada colaboradores que executar cargo considerado "função chave" haverá outro associado devidamente treinado e com senha de acesso aos mesmos sistemas, para substituição em situações de contingência.
Para fins exclusivos do presente Plano de Contingência e de Continuidade de Negócios, são consideradas funções chave:

(i) Administrador Fiduciário;
(ii) Colaboradores de BackOffice das áreas comerciais;
(iii) Colaboradores da área de Risco e Compliance;
(iv) Sócios (aqueles sócios com responsabilidades que envolvam tarefas críticas);
(v) Analista de TI Infra;
(vi) Colaboradores das áreas de Custódia, Controladoria e Controle de Fundos;
(vii)

10.1 SITUAÇÕES DE CONTINGÊNCIAS PREVISTAS

10.1.1 Ausência de colaboradores Chave por greves

Compreende as situações de greves de caráter trabalhista, de transportes públicos e etc.
Contingências existentes:

No caso de greve dos transportes, a AZUMI instruiu seus colaboradores a utilizar os serviços das cooperativas de táxi ou outros meios de transporte privado, como táxis ou carros de aluguel, com reembolso garantido para suprir a despesa.
Alternativamente, aqueles que não obtiverem sucesso na locomoção até o site principal, poderá acionar a contingência remotamente.
Procedimentos:

Responsável: Colaborador chave ou substituto ou COMITÊ de CONTINGÊNCIA.
Ativação da contingência:

Em caso de greve de transportes públicos, os colaboradores e substitutos devem procurar os meios de transporte privados a fim de chegar às dependências o mais rápido possível.
Em caso de ausência de funcionário chave, o respectivo substituto deverá realizar todas as tarefas necessárias para conclusão do processo de liquidação financeira das operações realizadas.
Em situações que obriguem o deslocamento para a AZUMI ou o acesso remoto, os colaboradores e seus substitutos serão deslocados até que todas as operações passem a ser realizadas através da contingência off-site.
Em caso de impedimento total de entrada na sede da AZUMI, o COMITÊ de CONTINGÊNCIA dividirá os colaboradores por acesso remoto, atentando que deverão ser encaminhados minimamente os colaboradores-chave descritos o item de CONTINGÊNCIA de PESSOAS.
No caso de alguns os colaboradores retornem para suas residências, utilizando as ferramentas de webmail, celulares com serviço de e-mail e acesso remoto à rede (este último recurso ainda em uso muito restrito) que permitem que os colaboradores possam realizar tarefas fora do ambiente do escritório através de uma conexão VPN de alta criptografia.

Retorno à normalidade:

No caso de necessidade de deslocamento físico, a retomada será feita mediante eliminação dos efeitos motivadores da contingência. Tão logo seja possível, o COMITÊ de CONTINGÊNCIA avisará aos colaboradores o retorno às instalações da AZUMI.

10.1.2 Ausência de Colaboradores Chave por Licença Médica ou Maternidade / Paternidade

Compreende as situações de ausências de associados em virtude de doenças ou licenças maternidade ou paternidade.

Contingências existentes:

Os casos de ausência por licenças serão analisados caso a caso, podendo o sócio ou diretor responsável pela área optar pelas seguintes providências:

- Deslocamento de um colaborador para treinamento das funções exercidas pelo (a) colaborador (a) licenciado (a);
- Contratação de um funcionário temporário em substituição.

Procedimentos:

Responsável: Sócio ou Diretor da área do colaborador

Ativação da contingência:

Licença maternidade
Durante o período gestacional, será definida a pessoa chave que assumirá as responsabilidades e tarefas da funcionária em licença maternidade. O sócio ou diretor da área decidirá se haverá a necessidade de novas contratações para suprir a ausência da associada. Durante o período de licença é ativada uma mensagem de “Out of Office” da Microsoft para que e-mails importantes não fiquem sem resposta. Na referida mensagem são descritos os períodos de ausência e quem contatar durante o mesmo.
Os acessos aos sistemas integrados à autenticação de rede serão bloqueados a partir da data de entrada em licença maternidade, exceto para casos de solicitação pela licenciada de utilização de webmail e/ou acesso remoto à rede, quando o login ficará ativo. Este controle é feito através de um check list de licença do Recursos Humanos
Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.
Licença paternidade
Durante os dias de licença paternidade as funções do funcionário serão assumidas pela equipe da área. Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.
Licença médica
O sócio da área definirá como será a substituição da pessoa chave de licença médica, que dependerá do período de ausência do associado chave e da gravidade do motivo da licença. O sócio ou diretor da área decidirá se haverá a necessidade de novas contratações para suprir a ausência do colaborador.
Os acessos aos sistemas integrados à autenticação de rede serão bloqueados a partir da data de entrada em licença médica, exceto para casos de solicitação pelo(a) licenciado(a) de utilização de webmail e/ou acesso remoto à rede, quando o login ficará ativo. Este controle é feito através de um check list de licença do DP.
Em caso de procurador, o restante do quadro de procuradores é suficiente para suprir a demanda.

11 CONTINGÊNCIAS DE INFRAESTRUTURAS TECNOLÓGICAS

ESTRUTURA DISPONIBILIZADA

A contingência de infraestrutura da AZUMI é padronizada em 3 principais pilares, são eles; Elétrico, Físico e Lógico.

Elétrico

Em caso de queda ou instabilidade na rede elétrica, o parque de máquinas da Azumi conta com (1) nobreak de 1200 va por estação de trabalho e garante uma autonomia média de 2h40m, o Data Center é servido por (2) nobreaks de 3 kva e oferece uma autonomia de até 8 horas para continuidade de sua operação.

Físico

De acordo com o que já foi mencionado, a AZUMI contará com ambiente em Cloud de contingência para a continuidade da operação, esta infraestrutura em Cloud com OpenVPN Connect permite o acesso remoto com garantia:

1. Alta Segurança

- Criptografia Forte: Utiliza criptografia AES-256, considerada altamente segura, para proteger os dados transmitidos.
- Autenticação Robusta: Suporta certificados digitais e autenticação de dois fatores (2FA), garantindo que somente usuários autorizados possam acessar a VPN.

2. Compatibilidade Multiplataforma

- Ampla Compatibilidade: Funciona em diversas plataformas, incluindo Windows, macOS, Linux, Android e iOS, permitindo que os usuários se conectem a partir de quase qualquer dispositivo.

3. Confiabilidade e Estabilidade

- Conexões Estáveis: OpenVPN Connect é conhecido por sua capacidade de manter conexões estáveis, mesmo em redes de baixa qualidade ou altamente congestionadas.
- Capacidade de Reconeção Automática: Se a conexão for perdida, o cliente pode reconectar automaticamente, minimizando a interrupção.

4. Facilidade de Uso

- Interface Simples: A interface do OpenVPN Connect é intuitiva, facilitando a conexão à VPN mesmo para usuários com menos experiência técnica.

Lógica

Para a contingência lógica a AZUMI conta com o plano de DRP (Desastre Recovery) para as seguintes Ci's; redundância para o link de internet principal de forma transparente e controlado pelo Firewall de borda SonicWall TZ500, utilizando o recurso de failover (quando identificado qualquer

anomalia no link principal, e para garantir a continuidade de operação o sistema aciona o link secundário automaticamente), redundância para o ambiente de dados e aplicações do servidor de produção para o ambiente de dados em cloud na RTM já supra mencionado, plano de backup e restore de dados (arquivos, pastas, arquivos de banco de dados) copiados regularmente em cloud AWS e Azure gerenciado com o software Veam backup, para o planejamento de backup está previsto 3 fases de cópias. Na primeira fase a cópia será realizada em Sharepoint + Microsoft Azure com a gestão de um backup completo mensal e outro incremental diário, na segunda fase será realizado uma vez por semana a cópia do primeiro backup em cloud Azure. Já na terceira e última fase será realizada uma cópia em tempo real do file server para o sistema Amazon AWS.

11.1 SITUAÇÕES DE CONTINGÊNCIAS PREVISTAS

11.1.1 Falha em servidor de arquivos e banco de dados

Contingências existentes:

Servidor de contingência com replicação on-line (ambiente Cloud Link RTM); Plano de backup

restore, backup completo + incremental até a data anterior ao incidente;

Procedimentos:

Responsável: Diretor de Tecnologia e responsável de TI INFRA
Ativação da contingência em caso de falha de hardware e/ou software:

- A área de TI INFRA acionará o serviço de contingência e a continuidade dos trabalhos passará ser realizada pelo site backup.
- Enquanto os funcionários trabalham no ambiente de contingência a equipe de TI INFRA ficará responsável por refazer os ambientes do servidor e restaurar o backup.
-

Retorno ao ambiente de produção em caso de falha de hardware e/ou software:

O retorno do ambiente de contingência para a produção deverá ocorrer na próxima noite em que este ambiente se encontrar disponível, após realização da restauração de backup, os dados serão atualizados de acordo com o último versionamento do ambiente de contingência.
Depois de restabelecido o ambiente de produção, serão reativados os processos de replicação e standby.

11.1.2 Falha no Banco de Dados SQL

O Banco de Dados SQL abriga as bases de sistemas, em sua maioria de terceiros, que são desenvolvidos em cima desta plataforma:
Sinqia

Contingências existentes:

Servidor de contingência com replicação on-line (ambiente Cloud Link RTM); Plano de backup

restore, backup completo + incremental até a data anterior ao incidente;

Procedimentos:

Responsável: Diretor de Tecnologia e responsável de TI INFRA

Ativação da contingência em caso de falha de hardware e/ou software:

- A área de TI INFRA acionará o serviço de contingência e a continuidade dos trabalhos passará ser realizada pelo site backup.
- Depois de concluída a ativação da contingência, a área de TI INFRA informará aos usuários, devendo estes se conectar novamente à instância do banco de dados através dos sistemas, dando continuidade as tarefas do ponto onde haviam sido interrompidas. Durante o período em que o servidor de contingência estiver operando como produção, a equipe de TI trabalhará na restauração dos serviços na reconstrução de ambientes e restauração dos dados.

Retorno ao ambiente de produção em caso de falha de hardware e/ou software:

O retorno do ambiente de contingência para a produção deverá ocorrer na próxima noite em que este ambiente se encontrar disponível, após realização da restauração de backup, os dados serão atualizados de acordo com o último versionamento do ambiente de contingência.
Depois de restabelecido o ambiente de produção, serão reativados os processos de replicação e standby.

11.1.3 Falha na Rede - Switch

Contingências existentes:

A estrutura atual conta com uma contingência de barramento duplo, onde cada switch possui dois caminhos distintos para o switch de borda (principal). Em caso de queda de uma das conexões, a segunda entra em atividade automaticamente, evitando assim a perda de pacotes.
Procedimentos:

Responsável: Diretor de Tecnologia e responsável de TI INFRA
Ativação da contingência em caso de falha de hardware e/ou software:

A equipe de TI será notificada via Zabbix e verificará o motivo da falha e deverá tomar as devidas providências para correção que dependerão do problema ocorrido.
Problemas físicos na conexão - verificação se existe mal contato ou refazer o cabo se necessário;
Problemas físicos na porta do switch – desativação da porta danificada e a substituição do ponto físico para outra porta livre. Após esse procedimento, providenciar a manutenção do equipamento em questão junto ao fabricante;
Problemas físicos no equipamento – remanejamento dos pontos para portas livres nos outros switches.

Retorno ao ambiente de produção

A equipe de TI INFRA retornará com o equipamento após a manutenção, restabelecendo todas as conexões após o fechamento dos sistemas.

11.1.4 Falha no Sistema de Refrigeração da Sala dos Servidores/Equipamentos Data Center

A sala dos servidores abrange todos os servidores
Contingências existentes:

Dois equipamentos de ar-condicionado que ficam ligados 24 horas.
Responsável: Diretor de Tecnologia e responsável de TI INFRA
Ativação da contingência em caso de falha de hardware e/ou software:

O segundo equipamento de ar permanecerá ligado, devendo a equipe de TI INFRA providenciar a manutenção do equipamento, com a qual possuímos um contrato de manutenção e prevenção para a solução do problema.
Retorno ao ambiente de produção

A equipe de TI INFRA ativará o equipamento envolvido assim que o mesmo estiver consertado

12 CONTINGÊNCIAS DE SERVIÇOS EXTERNOS

O AZUMI identificou os serviços listados a seguir como críticos, levando em conta dois aspectos: relevância do serviço prestado e/ou prestadores de serviços com excessiva concentração no mercado:

- Manutenção de posições de clientes;
- Liquidação de operações com clientes;
- Serviços de administração de fundos;
- Informações cadastrais;
- Gerenciamento de documentos.

12.1 SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

12.1.1 Manutenção de posições de clientes

Sinqia

Fromtis

Contingências existentes:

Geração de relatório do sistema Sinqia comparando com relatório de Custódia do dia anterior;

Colaboradores da área de custódia poderão acessar o sistema em nuvem da Sinqia diretamente de suas posições no site de contingência da RTM, uma vez que a aplicação é Web está alocado nas dependências de sua fabricante também amparado por redundâncias.

Responsável: Diretor de Custódia e Diretor de Operações

Em caso de falha acionar a empresa prestadora do serviço.

12.1.2 Liquidação de operações com clientes

Sinqia

Fromtis

Banco liquidante (a definir)

Contingências existentes:

Colaboradores da área de custódia poderão acessar o sistema Web da Sinqia diretamente em trabalho home-office ou coworking, uma vez que a aplicação é
Web está alocado nas dependências de sua fabricante também amparado por redundâncias.
Referente a liquidação os colaboradores chave podem acessar o ambiente de contingência através de **OpenVPN Connect e autenticação** multifator (MFA)

Todos os serviços estão descritos e amparados por contratos.

Responsável: Diretor de Custódia e Diretor de Operações

Em caso de falha acionar a empresa prestadora do serviço.

12.1.3 Serviços de administração de fundos

Sinqia

Fromtis

Contingências existentes:

Colaboradores da área de custódia poderão acessar o sistema Web da Sinqia e Fromtis diretamente em trabalho home-office ou coworking, uma vez que a aplicação é Web está alocado nas dependências de sua fabricante também amparado por redundâncias.

Planilhas de contingência formatadas pela AZUMI e individualizadas por tipo de operação com envio por e-mail; para que os gestores enviem as operações dos fundos e cotistas;

Planilha interna de dupla checagem para as operações da carteira; Planilhas de

contingência de movimentação de cotistas.

Controle em planilha paralela para a carteira e apuração da cota;

Para cotistas existe a impressão diária de relatório de fechamento de posição dos cotistas. Em caso de aplicação, aguarda-se o retorno do sistema dentro do dia, mas considera-se a entrada de financeiro na planilha de caixa (controle paralelo);

Em caso de resgate, atualiza-se a cota em uma planilha com a posição dos clientes, e então calcula-se o resgate que será pago assim como o imposto da operação.

Todos os serviços estão descritos e amparados por contratos.

Responsável: Diretor de Custódia e Diretor de Operações e Diretor Comercial

Em caso de falha acionar a empresa prestadora do serviço.

12.1.4 Informações cadastrais

Software Cadastro Único

Contingências existentes:

Colaboradores da área de cadastro e compliance e deveram acessar a contingência, onde o servidor de VPN está conectado no Software Cadastro Único
e poderão fazer suas rotinas de manutenção de posição normalmente.

Todos os serviços estão descritos e amparados por contratos.

Responsável: Diretor de Operações e Diretora de Compliance

Em caso de falha acionar a empresa prestadora do serviço.

12.1.5 Gerenciamento de documentos

Software Cadastro Único, RISC (Advice) e Fromtis

Custódia da documentação física contábil, fiscal e contratual; documentação cadastral de clientes contrato assinado, serão armazenamento da digitalização nos sistemas; e este armazenamento possui backup, bem como outras mídias eletrônicas.

Todos os serviços estão descritos e amparados por contratos.

Contingências existentes:

Fromtis e Software Cadastro Único: O ambiente de contingência será instalado nos servidores Amazon AWS.
RISC (Advice): O ambiente de contingência será instalado nos servidores Oracle.

Responsável: Diretor de Custódia e Diretor de Operações

Em caso de falha acionar a empresa prestadora do serviço.

ANEXO 1 – PLANO DE CONTATO

Todos os usuários dos grupos de aprovação, em caso de contingência, são responsáveis por autenticação multifator (MFA) e senhas dos sistemas para que possam proceder as aprovações de fora do ambiente da AZUMI.

ANEXO 2- CRONOGRAMA DE TESTES

CUSTÓDIA, CONTROLADORIA,

Primeiro sábado dos meses de dezembro e junho.

ANEXO 3- DENIFINIÇÃO DE PRIORIDADES

Em caso de contingência total todos os sistemas da AZUMI serão rodados nos sites de contingência descritos acima, para que esta situação não tenha nenhum impacto para os clientes existem alguns sistemas que deverão entrar em contingência imediatamente, para que evite demora devido ao excesso de dados.

Os sistemas elencados são primordiais para manter todas as operações em funcionamento sem que nenhum impacto seja sentido pelos clientes:

Cadastro Único, SINQIA, FROMTIS e RTM (site contingência e link dedicado).

INFORMES AOS CLIENTES

Para que tenhamos certeza de que nossos clientes não serão impactados iremos informar os telefones para contato e os procedimentos caso necessário para que possam fazer as operações normalmente, por e-mail. Adicionalmente, no site da AZUMI serão incluídos avisos com as informações necessárias para que os clientes mantenham o dia a dia normalmente.

Em caso de contingência na liquidação das operações, as contrapartes serão informadas através de contato telefônico e aviso no Sisbacen.

13 INFORMAÇÕES SOBRE O DOCUMENTO

1. Periodiocidade de revisão desse documento	1 ano	(X) Peridiocidade prevista em regulamentação ( ) Peridiocidade definida internamente
2. Necessidade de divulgação do documento no site da Internet da AZUMI DTVM	( ) Sim (X) Não	

3. Documento é para atendimento de regulamentação especifica	(X) Sim ( ) Não
	Resolução Bacen nº 4.893, de 26 de fevereiro de 2021