

**POLÍTICA DE SEGREGAÇÃO,
CONFIDENCIALIDADE, SEGURANÇA DA
INFORMAÇÃO E SEGURANÇA
CIBERNÉTICA**

**MZM WEALTH PLANNING CONSULTORIA
DE VALORES MOBILIÁRIOS LTDA.**

Março-2021
Versão 1.2

ÍNDICE

INTRODUÇÃO E OBJETIVO	3
CONFIDENCIALIDADE	3
Procedimentos internos para tratar eventual vazamento de informações confidenciais, reservadas ou privilegiadas	4
SEGURANÇA DA INFORMAÇÃO	5
A. Aspectos Gerais	5
B. Testes Periódicos	6
SEGREGAÇÃO DE ATIVIDADES	6
PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA	9
A. Identificação e avaliação de riscos (<i>risk assessment</i>)	9
B. Ações de prevenção e proteção	9
C. Plano de resposta	11
D. Reciclagem e revisão	12
PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS	12
A. Objetivo	12
B. Principais riscos potenciais mapeados	12
C. Respostas do PCN	13
D. Medidas de Prevenção	13
E. Teste de Contingência	13
REVISÕES, ATUALIZAÇÕES E VIGÊNCIA	14

INTRODUÇÃO E OBJETIVO

A presente Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética da MZM Wealth Planning Consultoria de Valores Mobiliários Ltda. (“MZM Wealth Planning” ou “Consultora”) tem por objetivo descrever os procedimentos observados pela Consultora para garantir a devida segregação, confidencialidade e segurança das informações e segurança cibernética, para fins de atendimento ao disposto na regulamentação vigente.

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética se aplica aos sócios, administradores, funcionários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da MZM Wealth Planning (“Colaboradores”).

CONFIDENCIALIDADE

Todas as informações que se referem a sistemas, negócios, estratégias, posições ou a clientes da MZM Wealth Planning são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na MZM Wealth Planning e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes da MZM Wealth Planning deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, por escrito, salvo na hipótese de decisão judicial específica que determine à Consultora a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório da Comissão de Valores Mobiliários (“CVM”). Caso a MZM Wealth Planning ou qualquer dos Colaboradores sejam obrigados a revelar as informações de clientes em face de procedimento judicial ou extrajudicial da CVM, tal fato deve ser comunicado aos clientes afetados, salvo se de outra forma estabelecido pelo órgão fiscalizador.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura venham a trabalhar junto à MZM Wealth Planning mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou da própria Consultora. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à administração da MZM Wealth Planning, para que sejam tomadas as medidas cabíveis.

A MZM Wealth Planning exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Consultora, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

O material com informações de clientes ou de suas operações deverá ser mantido nas dependências da Consultora, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa, por escrito, do Diretor de *Compliance* e PLDFT, conforme definido no contrato social da Consultora. Ainda, os arquivos eletrônicos recebidos ou gerados pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo da área, do cliente ou do projeto a que se refere tal arquivo eletrônico.

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade da Consultora, presente no Anexo II da Política de Regras, Procedimentos e Descrição dos Controles Internos da Consultora, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando na Consultora e durante certo período após terem deixado a MZM Wealth Planning.

Para fins de manutenção das informações confidenciais, a MZM Wealth Planning recomenda que seus Colaboradores (i) bloqueiem o computador quando o mesmo não estiver sendo utilizado ou estiverem ausentes da sua estação de trabalho, (ii) mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro, (iii) descartem materiais usados, destruindo-os fisicamente, e (iv) jamais revelem a senha pessoal de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

Procedimentos internos para tratar eventual vazamento de informações confidenciais, reservadas ou privilegiadas

Não obstante todos os procedimentos e aparatos tecnológicos adotados pela Consultora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Consultora (“Informações” ou “Informação”), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de *Compliance* e PLDFT deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de *Compliance* e PLDFT, primeiramente, identificará se a Informação vazada se refere às informações de produtos de investimento ou prestadores de serviços recomendados ou aos dados pessoais de seus clientes. Realizada a identificação, o Diretor de *Compliance* e PLDFT procederá da seguinte forma:

1. No caso de vazamento de informações relativas aos produtos de investimento ou prestadores de serviço recomendados:

Imediatamente, o Diretor de *Compliance* e PLDFT informará ao agente responsável por resguardar as Informações referentes aos produtos de investimento ou aos prestadores de serviços recomendados, nos termos da regulamentação vigente, para que este tome as medidas necessárias visando afastar eventuais danos ou prejuízos que possam vir a originados pelo vazamento das Informações, como, por exemplo, a publicação de fato relevante, nos

termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação.

2. No caso de vazamento de Informações relativas aos clientes:

Neste caso, ao Diretor de *Compliance* e PLDFT procederá com o tanto necessário para cessar a disseminação da Informação ou atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados na matéria; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, o Diretor de *Compliance* e PLDFT ficará à inteira disposição para auxiliar na solução da questão.

SEGURANÇA DA INFORMAÇÃO

A. Aspectos Gerais

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos clientes ou do acompanhamento das operações a eles relacionadas, ficam armazenadas na sede da Consultora, com *backup* de dados. O acesso aos arquivos é permitido apenas aos diretores da MZM Wealth Planning, ou aos Colaboradores previamente por eles autorizados.

Todo *software* disponibilizado aos Colaboradores deverá ser utilizado somente para os negócios da Consultora, em consonância com os acordos de licenciamento firmados.

O acesso aos sistemas de informação da Consultora é feito por meio de um par “usuário/senha”. O acesso e o uso de qualquer informação, pelo usuário, deve se restringir ao necessário para o desempenho de suas atividades profissionais no âmbito da Consultora. O controle desses dados é de domínio da MZM Wealth Planning, uma vez que o armazenamento dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

Para acessar informações nos sistemas da Consultora deverão ser utilizadas somente ferramentas e tecnologias autorizadas e previamente estabelecidas pela MZM Wealth Planning, de forma a permitir a identificação e rastreamento de quais usuários tiveram acesso a determinadas informações (os logs de acesso ficam armazenados nos sistemas).

Adicionalmente, informamos que a rede da Consultora é composta por diretórios de dois níveis: (i) diretórios de informações públicas, aos quais todos os Colaboradores têm acesso, contendo tão somente informações de natureza administrativa; e (ii) diretórios de acesso restrito, cujo acesso é somente pré-autorizado pelo Diretor de *Compliance* e PLDFT aos membros de alguns departamentos específicos, em todos os casos sendo necessário o login e senha de cada integrante.

Todo Colaborador que tiver acesso aos sistemas de informação da MZM Wealth Planning é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não os divulgar a terceiros em qualquer hipótese.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Colaborador da Consultora.

A MZM Wealth Planning se reserva o direito de proibir o uso de telefones celulares na área de consultoria e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, como os arquivos armazenados ou criados pelos recursos da informática pertencentes à MZM Wealth Planning ou utilizados em nome dela, a fim de assegurar o fiel cumprimento desta política de Segurança da Informação, bem como da legislação em vigor.

B. Testes Periódicos

Periodicamente, a Consultora realiza testes de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- (i) Verificação semestral do login dos Colaboradores;
- (ii) Anualmente, altera-se a senha de acesso dos Colaboradores;
- (iii) Testes trimestrais no *firewall*;
- (iv) Testes semestrais nas restrições impostas aos diretórios;
- (v) Manutenção semestral de todo o *hardware* por empresa especializada em consultoria de tecnologia de informação;
- (vi) Testes quinzenais no *backup* (salvamento de informações), realizado na nuvem.

SEGREGAÇÃO DE ATIVIDADES

Visando atribuir o mais elevado grau de transparência, salienta-se que o Sr. Daniel Chiavenato Mazza, sócio da MZM Wealth Planning e Diretor de Consultoria e *Suitability*, presta o serviço de assessoria para fins de planejamento financeiro e patrimonial, através da Daniel Chiavenato Mazza – ME, inscrita no CNPJ/ME sob o nº 19.130.578/0001-90. Nesse sentido, cumpre ressaltar que a atividade de planejamento financeiro e patrimonial não se trata de atividade relacionada ao mercado financeiro e de capitais e, portanto, não está sujeita à regulação e fiscalização da CVM, motivo pelo qual não é suscitada qualquer hipótese de conflito de interesses entre atividades prestadas pela MZM Wealth Planning e a Daniel Chiavenato Mazza – ME.

Além da Daniel Chiavenato Mazza – ME, o Sr. Daniel Chiavenato Mazza é sócio de outras duas empresas, (i) a Guedes e Mazza Distribuidora Ltda. – ME, inscrita no CNPJ sob o nº

18.803.799/0001-10, cujo objeto social consiste, basicamente, na exploração do ramo de comércio atacadista de complementos e suplementos alimentícios e de cosméticos e produtos de perfumaria; e (ii) a Condomínio Village Villa 85 Empreendimento Imobiliário SPE Ltda., sociedade de propósito específico cujo objeto social consiste na incorporação, construção e comercialização de condomínio residencial (e, em conjunto com a Daniel Chiavenato Mazza – ME e a Guedes e Mazza Distribuidora Ltda. – ME, doravante denominadas “Outras Sociedades”).

Ademais, no mesmo endereço da MZM Wealth Planning funciona uma sociedade de agentes autônomos de investimentos. Não obstante, MZM Wealth Planning e a referida sociedade se instalam em espaços físicos completamente segregados, cujos acessos são controlados por intermédio de sistema eletrônico. Os Colaboradores não possuem autorização para adentrar ao espaço físico reservado à sociedade de agentes autônomos de investimentos, e vice-versa. Outrossim, a MZM Wealth Planning salienta, para todos os fins, que não possui qualquer nível de relação com a sociedade de agentes autônomos de investimentos em voga, seja de cunho societário ou comercial, de modo que, naturalmente, as empresas também possuem completa segregação lógica e funcional.

Sem prejuízo do previsto anteriormente, a MZM Wealth Planning adota as seguintes práticas centrais para eliminar ou mitigar eventuais conflitos, potenciais ou existentes:

I. Segregação Física, Lógica e Funcional

Inicialmente, cumpre ressaltar que a Consultora e as Outras Sociedades são completamente segregadas fisicamente.

Além disso existe a segregação lógica entre a Consultora e as Outras Sociedades, de modo que as empresas não compartilham recursos operacionais e tecnológicos, sendo os acessos aos diretórios completamente segregados, com controle individual de acesso, de forma a garantir o máximo nível de confidencialidade das informações e manter o sigilo devido das operações realizadas pela Consultora, conforme especificado na presente política. Ademais, salvo com relação ao Sr. Daniel Chiavenato Mazza, os demais Colaboradores da Consultora não atuam nas Outras Sociedades, sendo certo que, conforme exposto anteriormente, as empresas preservam a devida segregação exigida pela regulamentação vigente.

II. *Disclosure*:

A Consultora, sempre que necessário, dará *disclosure* aos seus clientes acerca da existência das Outras Sociedades.

Sem prejuízo, cumpre salientar, ainda, que para salvaguardar eventuais conflitos de interesse entre as áreas, todo e qualquer benefício recebido pela Consultora diretamente ou indiretamente em razão de suas recomendações, que não estejam previamente ajustados em instrumento contratual, serão integralmente revertidos aos seus clientes, conforme estabelecido na regulamentação em vigor.

Não obstante, no âmbito das atividades reguladas, a MZM Wealth Planning atua exclusivamente como consultora de valores mobiliários, não prestando, portanto, quaisquer outros serviços no mercado de capitais. Em razão disso, não é suscitada qualquer hipótese de conflito de interesses entre atividades prestadas pela Consultora. Não obstante, a MZM Wealth Planning manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

Ademais, a MZM Wealth Planning adota segregação interna. O primeiro nível de segregação dentro das atividades da MZM Wealth Planning refere-se às diferenças funcionais de atuação e autoridades definidas para as posições de consultores, *compliance* e administrativo. Perfis de acesso, e o controle são realizados com base nessas divisões.

O acesso de pessoas que não fazem parte do quadro de Colaboradores da Consultora será restrito à recepção e às salas de reunião ou atendimento, exceto mediante prévio conhecimento e autorização da administração da MZM Wealth Planning, e desde que acompanhadas de Colaboradores da Consultora. Em caso de antigos Colaboradores, não será permitida a sua permanência nas dependências da Consultora, com exceção dos casos em que tenha sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a clientes nas dependências da Consultora deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

As diferentes áreas da Consultora terão suas estruturas de armazenamento de informações logicamente segregadas das demais, de modo a garantir que apenas os Colaboradores autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma.

É importante ressaltar que a Consultora atualmente utiliza como sede imóvel projetado no estilo “coworking”, em que na mesma sede situam-se empresas com objetos sociais diversos. Sem prejuízo da característica do imóvel, a MzM WP possui espaço reservado para o desenvolvimento de suas atividades, sendo certo que será garantida à funcionalidade da Consultora a completa individualização com relação às demais atividades exercidas no respectivo imóvel.

Dentre os mecanismos a serem adotados, incluem-se o acesso restrito ao ambiente, através de crachás ou equipamentos que de forma semelhante garantam que somente serão aceitas as credenciais de seus Colaboradores, além da individualidade das chaves de acesso aos sistemas da Consultora.

Sem prejuízo, as regras destacadas na política de Segurança da Informação, tratada neste documento, sobretudo no que tange às segregações eletrônicas e de funções, se aplicam para fins da presente política de Segregação das Atividades, e devem ser observadas pelos Colaboradores da Consultora.

PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Responsável: Diretor de *Compliance* e PLDFT

A. Identificação e avaliação de riscos (*risk assessment*)

A Consultora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta, sendo que os ataques mais comuns de *cybercriminals* são:

- a) *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
- b) Engenharia Social;
- c) *Pharming*;
- d) *Phishing scam*;
- e) *Vishing*;
- f) *Smishing*;
- g) Acesso pessoal;
- h) Ataques de DDoS e *botnets*;
- i) Invasões (*advanced persistent threats*).

Com a finalidade de se manter resguardada contra estes e outros potenciais ataques, a Consultora definiu todos os ativos relevantes da instituição, fundamentais a seu funcionamento, criou regras para classificação das informações geradas e avalia continuamente a vulnerabilidade de cada um desses ativos.

A Consultora levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

B. Ações de prevenção e proteção

Uma importante regra de prevenção consiste na segregação de acessos a sistemas e dados que a Consultora adota, conforme já detalhado nas regras internas que tratam de Segurança da Informação e Segregação de Atividades.

A Consultora adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. A Consultora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis. A Consultora deve criar logs e trilhas de auditoria sempre que os sistemas permitam.

O acesso remoto a arquivos e sistemas internos ou na nuvem tem controles adequados, a critério do responsável pela Segurança Cibernética.

Outro ponto importante é que, ao concluir novos equipamentos e sistemas em produção, a Consultora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção. A Consultora conta com recursos *anti-malware* em estações e servidores de rede, como antivírus e *firewalls* pessoais. A Consultora deve, adicionalmente, proibir o acesso a determinados websites e a execução de *softwares* e/ou aplicações não autorizadas.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Consultora e circulem em ambientes externos à Consultora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. Qualquer exceção à presente regra deverá ser previamente autorizada por escrito pelo Diretor de *Compliance* e PLDFT.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Consultora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Consultora.

A utilização dos ativos e sistemas da Consultora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Consultora, bem como avisar prontamente o Diretor de *Compliance* e PLDFT.

Não obstante o disposto no parágrafo anterior, todos os anexos dos e-mails recebidos pelos Colaboradores da Consultora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A Consultora adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do plano de continuidade dos negócios da Consultora.

Os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

A Consultora possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. A Consultora mantém inventários atualizados de *hardware* e *software*, e verifica-os com frequência para identificar elementos estranhos à instituição.

A área responsável da Consultora deve diligenciar para manter os sistemas operacionais e *softwares* de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.

A área responsável deve também monitorar diariamente as rotinas de *backup*, executando testes regulares de restauração dos dados.

Deve-se, ademais, realizar testes de invasão externa, *phishing*, bem como análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

Os logs e trilhas de auditoria criados na forma definida no item anterior devem ser analisados regularmente pela área responsável, de forma a permitir rápida identificação de ataques, sejam internos ou externos.

C. Plano de resposta

A área de *compliance* deve elaborar um plano formal de resposta a ataques virtuais. A Consultora deverá estabelecer os papéis de cada área em tal plano, prevendo o acionamento de Colaboradores-chave e contatos externos relevantes.

O plano de resposta deverá levar em conta os cenários de ameaças previstos no *risk assessment*. Deve haver critérios para a classificação dos incidentes, por severidade. O plano deve prever, conforme o caso, o processo de retorno às instalações originais após o final do incidente, na hipótese em que as instalações de contingência ou acessos remotos tenham de ser utilizados.

D. Reciclagem e revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas da Consultora sobre a matéria, deverá ser revisto e atualizado anualmente.

Os grupos de trabalho diretamente envolvidos com qualquer parte do programa devem se manter atualizados, buscando fornecedores especializados, se necessário.

A Consultora deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

A. Objetivo

Com o objetivo de assegurar a continuidade dos negócios em eventos que impliquem na impossibilidade da operação normal em suas instalações principais, a MZM Wealth Planning possui uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada Colaborador na execução do Plano de Continuidade de Negócio (“PCN”).

O PCN é um plano traçado para que seja possível dar continuidade à execução de atividades consideradas críticas para a prestação de serviços pela Consultora, de forma que os interesses dos clientes da MZM Wealth Planning não sejam prejudicados.

O PCN estabelecido e sua ativação é responsabilidade do Diretor de *Compliance* e PLDFT. Periodicamente, o plano será revisado pelo Diretor de *Compliance* e PLDFT com a finalidade de: (i) verificar que o PCN esteja em concordância com as leis e normas dos órgãos reguladores e (ii) zelar por sua atualização e cumprimento do cronograma de treinamento previsto.

B. Principais riscos potenciais mapeados

A análise do impacto do negócio foi resumida para refletir os potenciais riscos que podem causar desastres, incidentes e consequentes possíveis perdas ao negócio da Consultora. São eles:

- a) Queda de energia.
- b) Queda do link para acesso à internet.
- c) Contingências para e-mail e rede de arquivos.
- d) Indisponibilidade do serviço de e-mail e rede de arquivos.
- e) Invasão da intranet por hackers.
- f) Impossibilidade de acessar o escritório

C. Respostas do PCN

Para os pontos “a”, “b” e “f”, a Consultora entende que a solução mais rápida é a utilização de outro computador de fora do escritório com acesso à internet.

Para o item “c”, o serviço de e-mail poderá ser acessado remotamente, garantindo a continuidade. Há possibilidade de comunicação nos celulares dos Colaboradores.

No item “d” e “e” o recomendado é utilizar a estação em nuvem, que possui acesso direto ao *backup* dos arquivos.

A implementação dos planos de contingência deverá ser realizada em até vinte e quatro horas e será de responsabilidade do Diretor de *Compliance* e PLDFT.

O reestabelecimento da operação poderá ser realizado por terceiros contratados e o prazo de ajuste será estimado pelo prestador de serviço em questão.

Adicionalmente, se necessário, a Consultora adotará soluções para:

- a) Substituir equipamentos danificados;
- b) Efetuar despesas contingenciais, incluindo a compra de equipamentos ou contratação de serviços que se fizerem necessários; e
- c) Avaliar os prejuízos decorrentes da interrupção das atividades regulares.

D. Medidas de Prevenção

A Consultora realiza o *backup* de seus dados semanalmente, possibilitando o acesso às últimas versões de cada arquivo para restauração (em caso de problemas ou solicitação do responsável pela área).

Os principais executivos da Consultora possuem acesso remoto aos seus e-mails, de modo que possam acessá-los de fora do escritório, se necessário. Os registros contábeis da Consultora ficarão com o contador responsável (terceirizado).

A equipe de consultoria da Consultora tem acesso a *softwares* que permitem a consulta do mercado financeiro em qualquer lugar do mundo.

E. Teste de Contingência

Será planejada a realização de testes de contingências anualmente, sob responsabilidade do Diretor de *Compliance* e PLDFT, sem prejuízo da implementação de testes que se façam necessários em uma menor periodicidade, de modo a possibilitar que a Consultora esteja preparada para a continuação de suas atividades. Tais testes devem ser realizados com o objetivo de verificar as condições para:

- a) Acesso aos sistemas;
- b) Acesso ao e-mail corporativo;
- c) Acesso aos dados armazenados em procedimento de *backup*; e
- d) Outros necessários à continuidade das atividades da Consultora.

O resultado de cada teste anual será registrado em relatório próprio obedecendo o disposto na regulamentação aplicável e as orientações das entidades responsáveis pela supervisão das atividades, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do presente PCN.

O PCN foi elaborado tendo em vista a possibilidade de realização de todos os trabalhos prestados pela Consultora sem dependência do acesso à sua localidade física.

REVISÕES, ATUALIZAÇÕES E VIGÊNCIA

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética será revisada, no mínimo, anualmente. Não obstante as revisões estipuladas, poderá ser alterado sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

A área de *compliance* informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Consultora na rede mundial de computadores.

Esta Política de Segregação, Confidencialidade, Segurança da Informação e Segurança Cibernética revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.