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

Versão 2.0
Revisado em: 03/06/2023

Atividade	Área
Elaboração	Área de *Compliance*
Revisão	Diretor de *Compliance* e Riscos
Aprovação	Diretor de *Compliance* e Riscos

Classificação das Informações
[ ] Uso Interno [X] Uso Público

Conteúdo

1. Apresentação

1.1. Introdução, Objetivo e Abrangência

Esta Política de Segurança da Informação, Confidencialidade, Segregação e Segurança Cibernética ("Política") se aplica à Actum Capital Gestão de Recursos Ltda. ("Actum Capital"), administradora de carteiras de títulos e valores mobiliários (Gestora) do Grupo Actum Capital, nos termos da resolução CVM nº 21, de 25 de fevereiro de 2021 e demais empresas do grupo.

A presente Política tem por objetivo descrever os procedimentos observados pelo Grupo Actum Capital para garantir a devida segregação, confidencialidade e segurança das informações e segurança cibernética, para fins de atendimento ao disposto na regulamentação vigente.

Esta Política se aplica a todos os sócios, diretores, empregados, funcionários, trainees, estagiários, prestadores de serviços que venham, de maneira direta ou indireta, trabalhar para a Actum Capital e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Actum Capital ("Membros").

1.2. Definições

A segurança da informação descrita nesta Política é caracterizada pela preservação dos seguintes conceitos:

- Confidencialidade: garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- Disponibilidade: garante que a informação esteja disponível para as pessoas autorizadas sempre que se fizer necessária;
- Integridade: garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

2. Responsabilidades

É missão e responsabilidade de cada Membro observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente Política. É imprescindível que cada Membro compreenda o papel da segurança da informação em suas atividades diárias. Todas as atividades executadas pelos Membros, devem observar a legislação vigente, a normatização de órgãos e entidades reguladoras e as regras internas do Grupo Actum Capital e as regras específicas da Gestora que o Membro esteja vinculado. A área de *compliance* é responsável por editar as políticas e padrões que apoiam a todos na proteção dos ativos de informação, e está preparado para auxiliar na resolução de problemas relacionados ao tema. Em caso de dúvidas, as mesmas poderão ser esclarecidas pela área de *compliance*, liderada pelo Diretor de *Compliance* e Riscos, conforme definido no contrato social vigente da Gestora.

3. Confidencialidade

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora do Grupo Actum Capital, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais. Incluem-se aqui, por exemplo, posições compradas ou vendidas, estratégias e conselhos de investimento ou de desinvestimento, relatórios, análises e opiniões sobre ativos financeiros, dados a respeito de resultados financeiros antes da publicação dos balanços e balancetes das empresas integrantes do Grupo Actum Capital e dos veículos de investimento cujas carteiras sejam geridas pela Gestora, transações efetuadas e que ainda não foram publicadas, informações oriundas de estudos efetuados pelas áreas da sociedade etc.

Qualquer informação sobre o Grupo Actum Capital, ou de qualquer natureza relativa às atividades desempenhadas pela Gestora, e aos Membros e clientes, obtida em decorrência do desempenho das atividades normais do Membro no Grupo Actum Capital, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado expressamente pelo Diretor de *Compliance* e Riscos. A solicitação e a concessão da autorização devem ser registradas por e-mail, que deverá ser armazenado por prazo não inferior a 5 (cinco) anos.

Não obstante o acima descrito, o Diretor de *Compliance* e Riscos e o Diretor de Gestão, conforme definido no contrato social vigente de cada Gestora, serão os únicos responsáveis diretos pela obtenção das informações relativas a análises de investimentos provenientes da empresa contratada pela Gestora. Tais informações não serão compartilhadas por nenhuma outra pessoa – Membro ou não –, o que impossibilita a utilização destas informações por pessoas não habilitadas em processo de decisão de investimento.

É terminantemente proibido que os Membros façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da(s) Gestora(s) a que tiver acesso e circulem em ambientes externos com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses do Grupo Actum Capital. Nestes casos, o Membro 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.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno do Grupo Actum Capital.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados semanalmente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão. As possíveis penalidades aplicáveis por descumprimento das regras internas do Grupo Actum Capital e específicas da Gestora estão descritas nesta Política e no Código de Ética e Manual de *Compliance*.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Membros devem se abster de utilizar *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no Grupo Actum Capital.

Os Membros, quando de sua contratação, devem assinar o Termo de Compromisso com o Código de Ética do Grupo Actum Capital, presente no Anexo I ao Código de Ética e Manual de *Compliance*, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações a que tiverem acesso enquanto estiverem trabalhando no Grupo Actum Capital.

Sem prejuízo dos procedimentos dispostos nesta seção, o Grupo Actum Capital orienta os seus Membros a tratar as informações adiante da seguinte forma:

Informação privilegiada

Pode-se considerar como informação privilegiada qualquer informação importante a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Membro.
São exemplos de informações privilegiadas: informações verbais ou documentadas referentes a resultados operacionais de empresa, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, e qualquer outro acontecimento que seja motivo de um acordo de confidencialidade fixado por uma empresa com o Grupo Actum Capital ou com terceiros.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Quem tiver acesso a uma informação privilegiada deverá transmiti-la rapidamente à área de *compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros Membros, profissionais de mercado, amigos e parentes, e nem a usar, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se rapidamente relatar o ocorrido ao *compliance officer*. Quem tiver acesso a uma informação privilegiada deverá reduzir ao máximo a circulação de documentos e arquivos com tal informação.

***Insider Trading* e "Dicas"**

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo o próprio Grupo Actum Capital e seus Membros).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

É proibida a prática dos casos mencionados anteriormente por qualquer Membro, seja agindo em benefício próprio, do Grupo Actum Capital ou de terceiros.

É de responsabilidade do *compliance officer* verificar e processar, trimestralmente, as notificações recebidas a respeito do uso pelos Membros de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas"

devem ser analisados não só durante a vigência do relacionamento profissional do Membro com o Grupo Actum Capital, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

3.1. Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, reservadas ou privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pelo Grupo Actum Capital para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora ("Informações" ou "Informação"), na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o Diretor de *Compliance* e Riscos deverá tomar ciência do fato tão logo seja possível.

De posse da Informação, o Diretor de *Compliance* e Riscos, primeiramente, identificará se a Informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de cotistas. Realizada a identificação, o Diretor de *Compliance* e Riscos procederá da seguinte forma:

No caso de vazamento de Informações relativas aos fundos de investimento geridos:

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

No caso de vazamento de Informações relativas aos cotistas:

Neste caso, ao Diretor de *Compliance* e Riscos 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 Riscos ficará à inteira disposição para auxiliar na solução da questão.

4. Segurança da Informação

A conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pela área de *compliance*, não terão acesso aos servidores e arquivos. Somente será possível em ambiente externo à rede.

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

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e/ou afetar a reputação do Grupo Actum Capital.

O *compliance officer* também será avisado por e-mail em caso de tentativa de acesso aos diretórios e logins virtuais no servidor protegidos por senha. O *compliance officer* elucidará as circunstâncias da ocorrência deste fato e comunicará ao Diretor de *Compliance* e Riscos a fim de se estudar eventual aplicação de sanções.

Em nenhuma hipótese um Membro pode emitir opinião por e-mail em nome do Grupo Actum Capital ou da Gestora, ou utilizar material, sua marca e logotipos para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado pelo Diretor de *Compliance* e Riscos para tanto.

Programas instalados nos computadores, principalmente via *internet* (*downloads*), sejam de utilização profissional ou para fins pessoais devem obter autorização prévia, por e-mail, do responsável pela área de informática. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente, por e-mail, ao responsável pela informática. Este deverá aprovar ou vetar, por e-mail, a instalação e utilização dos *softwares* dos Membros para aspectos profissionais e pessoais. A área de *compliance* deverá ser mantida em cópia na troca de e-mails ora referida.

A Gestora se reserva no direito de gravar qualquer ligação telefônica dos seus respectivos Membros realizada ou recebida por meio das linhas telefônicas disponibilizadas pela Gestora para a atividade profissional de cada Membro. O *compliance officer* é encarregado de, quinzenalmente, escutar, por amostragem, as ligações realizadas pelos Membros. Qualquer

informação suspeita encontrada será esclarecida imediatamente. As gravações poderão ser arquivadas pelo prazo de 180 (cento e oitenta) dias.

Todas as informações do servidor do Grupo Actum Capital, do banco de dados dos clientes etc. são enviados para o servidor interno. Nesse servidor, as informações são segregadas por Gestora e área e transformadas em pacotes criptografados, sendo armazenadas com *backup*.

4.1. Definição de Perfis de acesso aos sistemas, rede, base de dados e servidores

Inicialmente, conforme detalhado adiante nesta Política, é importante pontuar que a Gestora possuem ambiente de acesso segregados, de modo que as diferentes áreas das Gestora e Compliance e suas estruturas de armazenamento de informações logicamente segregadas das demais para garantir que apenas os Membros autorizados e necessários para o desempenho de determinada atividade tenham acesso às informações da mesma. Assim, garante-se que somente Membros de uma determinada área possuam acesso às informações de tal área, evitando a disseminação de informações sigilosas, sem prejuízo de eventual compartilhamento de informações necessárias à consecução das atividades da Gestora.
A definição dos perfis de acesso ao sistema, rede, base de dados e servidores, serão listados na Matriz de Perfis de Acesso, constando informações referentes a função e responsabilidade de cada usuário, a fim de evitar o contato com informações indevidas e/ou irrelevantes para o desempenho de suas funções profissionais.

Assim, fica vedada o compartilhamento de documentos e informações por pessoas não autorizadas a terceiros ou outros Membros, salvo se houver aprovação expressa, por e-mail, do Diretor de *Compliance* e Riscos nesse sentido. Qualquer conduta não autorizada na transferência de informações estará sob pena de aplicação de sanções disciplinares e legais.

É importante ressaltar que os acessos acima referidos são imediatamente cancelados em caso de desligamento do Membro do Grupo Actum Capital.

4.2. Acesso Físico

É vedado aos Membros que não tenham autorização o acesso ao ambiente físico designado ao setor de gestão da Gestora, bem como aos equipamentos de informática e demais equipamentos e sistemas utilizados que somente serão acessíveis através de senha pessoal aos Membros autorizados.

4.3. Regras para definição/alteração de senha

Como medida de segurança, o cadastramento ou alteração de senhas deve satisfazer a requisitos de complexidade, reduzindo assim riscos de acesso ou invasão de pessoas não autorizadas às informações internas. Este conceito se aplica aos acessos via Office 365.

As senhas precisarão atender os seguintes requisitos:

- Não conter partes significativas do nome da conta do usuário ou o nome todo
- Ter pelo menos oito caracteres de comprimento
- Conter caracteres de três das quatro categorias a seguir:
    - Caracteres maiúsculos (A-Z)
    - Caracteres minúsculos (a-z)
    - Dígitos básicos (0-9)
    - Caracteres não-alfabéticos (por exemplo, !, $, #, %)

4.4. Regras para uso da Internet

O acesso à Internet deverá ser utilizado apenas para desenvolvimento das atividades profissionais pertinentes a área e função de cada Membro, não sendo permitidos acessos para outros fins, exceto em casos específicos, desde que com autorização prévia, por e-mail, do Diretor de *Compliance* e Riscos.

Não é permitido aos usuários o acesso a páginas da impróprias, com conteúdo pornográfico ou material relacionado, qualquer outro aspecto ilegal ou em desacordo com as diretrizes internas do Grupo Actum Capital.

4.5. Regras de Download

Não é permitido o "download" ou cópia de material da Internet, sem a devida necessidade e autorização prévia, por e-mail, da área de informática, com cópia para a área de *compliance*. Nos casos em que haja a autorização, deverá ser assegurada a propriedade intelectual e os direitos autorais do seu proprietário.

4.6. Regras para Upload

Os usuários não deverão divulgar na internet qualquer material que possa ser considerado impróprio, ofensivo ou desrespeitoso, ou que de alguma maneira, possam comprometer a

imagem do Grupo Actum Capital, devendo cada Membro estar ciente e em conformidade com as diretrizes internas do Grupo Actum Capital.

4.7. Utilização do E-mail Corporativo

O uso do e-mail corporativo será exclusivo para questões profissionais de cada Membro, não sendo permitido a utilização do mesmo para questões pessoais, devendo todos seguirem as seguintes regras:

- Utilizar o e-mail coorporativo, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, política e normas vigentes;
- Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;
- Não enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Não se ausentar da estação de trabalho sem bloquear a máquina, garantindo assim a impossibilidade de acesso indevido por terceiros;
- Não revelar a senha de acesso à rede corporativa, computadores, Internet e/ou de sua caixa postal (e-mail) coorporativo a ninguém e tomar o máximo de cuidado para que ela permaneça somente sob seu conhecimento;
- Não enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Alterar sua senha, sempre que obrigatório ou que tenha suspeição de descoberta por terceiros, não usando combinações simples que possam ser facilmente descobertas, com base na seção “Regras para definição/alteração de senha” presente nesta Política;
- Não apagar mensagens pertinentes de correio eletrônico quando o Grupo Actum Capital ou gestora estiver sujeita a algum tipo de investigação;
- Responder, em todas as instâncias, pelas consequências das ações ou omissões de própria parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de sua senha ou das transações a que tenha acesso.

4.8. Tratamento do espaço disponível da rede

É de responsabilidade do Membro a manutenção de sua pasta de rede, bem como área de trabalho, devendo fazer a exclusão ou o arquivamento dos arquivos em outro local apropriado com intuito de manter espaço livre. Recomenda-se a utilização da pasta própria criada com o nome do Membro na aba "Este Computador", já que os arquivos salvos na área de trabalho podem ser perdidos em eventual pane no computador ou em eventual limpeza de rede para liberação de espaço.

A pasta de Rede "Actum Capital" deverá ser acompanhada pela área de *compliance*, devendo esta monitorar o espaço livre, impedindo que o diretório fique completamente cheio e cause problemas no fluxo de trabalho das áreas. Sempre que o espaço livre for inferior à 5 Gigas, será realizada uma limpeza das pastas, de modo a otimizar o espaço disponível.

4.9. Metodologia de *Backup*

Todas as informações da rede de acesso do Grupo Actum Capital são enviadas para o servidor interno diariamente. Nesse servidor, as informações são segregadas por áreas da Gestora, Compliance e demais áreas e pastas do grupo, sendo armazenadas com *backup* realizado por empresa terceirizada, em tempo real, em serviço de *backup* na nuvem com acesso somente ao administrador de rede.

4.10. Testes Periódicos

Periodicamente, o Grupo Actum Capital 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 Membros;
(ii) Anualmente, altera-se a senha de acesso dos Membros;
(iii) Testes semestral 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 no *backup* (salvamento de informações) na periodicidade estabelecida no item "Metodologia de *Backup*" acima.

4.11. Violação da Política, Normas e Procedimentos de Segurança da Informação

As violações de segurança devem ser informadas à área de *compliance*, por meio de e-mail, com todas as informações relativas ao fato ocorrido. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos.

Exemplos que podem ocasionar riscos operacionais ou sanções:

- Uso ilegal de *software*;
- Introdução (intencional ou não) de vírus de informática;
- Tentativas de acesso não autorizado a dados e sistemas;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas.

Os princípios de segurança estabelecidos na presente Política possuem total aderência do Conselho de Administração e devem ser observados por todos na execução de suas funções. A não-conformidade com as diretrizes desta Política e a violação de normas derivadas da mesma sujeita os Membros às penas de responsabilidade civil e criminal na máxima extensão que a lei permitir e a rescisão de contratos. Em caso de dúvidas quanto aos princípios e responsabilidades descritas nesta Política, os Membros devem entrar em contato com a área de *compliance*.

5. Propriedade Intelectual

A propriedade intelectual é composta por bens imateriais, tais como: marcas, sinais distintivos, slogans publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio). Quaisquer informações e propriedade intelectual que pertençam ao Grupo Actum Capital, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

6. Procedimentos de Segurança Cibernética

Responsável: Diretor de *Compliance* e Riscos

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

O Grupo Actum Capital deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Guia ANBIMA de Segurança Cibernética definiu que os ataques mais comuns de cybercriminals são os seguintes:

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, o Grupo Actum Capital 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.

O Grupo Actum Capital levou também em consideração os possíveis impactos financeiros, operacionais e reputacionais em caso de evento de segurança.

6.2. Ações de prevenção e proteção

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

O Grupo Actum Capital adota, além disto, regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância do ativo acesso. Grupo Actum Capital 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. O Grupo Actum Capital 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, o Grupo Actum Capital 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. O Grupo Actum Capital conta com recursos anti-malware em estações e servidores de rede, como anti-virus e firewalls pessoais.

É terminantemente proibido que os Membros façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da(s) Gestora(s) a que tiver acesso e circulem em ambientes externos com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Membro 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 Membros devem se abster de utilizar *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade no Grupo Actum Capital.

Todos os anexos dos e-mails recebidos pelos Membros são rigidamente verificados pelos servidores, de modo que os Membros sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

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

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

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

O Grupo Actum Capital adota também *backup* das informações e dos diversos ativos da instituição, conforme as disposições do presente documento.

Os Membros 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 ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com a resolução CVM 21/2021 e Resolução CVM nº 50/2021, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.
O Grupo Actum Capital possui mecanismos de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade.

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

A área de informática 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.

6.3. Plano de resposta

A área de *compliance* deve, conjuntamente com os profissionais da área de informática, elaborar um plano formal de resposta a ataques virtuais. O Grupo Actum Capital deverá estabelecer os papeis de cada área em tal plano, considerando as atividades da Gestora, se for o caso, prevendo o acionamento de Membros-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.

6.4. Reciclagem e revisão

O programa de segurança cibernética, que contempla os procedimentos aqui descritos, o plano formal de resposta e demais políticas internas do Grupo Actum Capital 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.

O Grupo Actum Capital deverá divulgar o programa de segurança cibernética internamente e disseminar a cultura de segurança, alertando sobre os riscos principais e as práticas de segurança.

7. Segregação de Atividades

Inicialmente, cumpre esclarecer que a Gestora, controladas pelo Grupo Actum Capital., atua exclusivamente como administradoras de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais.

As regras destacadas na seção “Segurança da Informação” se aplicam para fins da presente política de Segregação de Atividades, e devem ser observadas pelos Membros.

Procedimentos adicionais visando a mitigação de potenciais conflitos de interesses podem ser consultados no Código de Ética e Manual de *Compliance*, disponível para consulta pública.

Ademais, no tocante às demais empresas do Grupo Actum Capital., não há que se falar em conflitos de interesses, uma vez que não são exercidas atividades conflitantes com aquelas desenvolvidas pela Gestora.

Por fim, o Diretor de *Compliance* e Riscos possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos administradores ou sócios do Grupo Actum Capital, salvo se for de competência do Comitê de *Compliance* e Risco.

8. Disposições Finais

O Grupo Actum Capital armazenará as evidências descritas nesta Política, incluindo, sem se limitar, o fluxo de e-mails, por prazo não inferior a 5 (cinco) anos.

Esta Política 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 Membros sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na rede mundial de computadores.

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.