

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

1. INTRODUÇÃO

A Política de Segurança das Informações e de Segurança Cibernética da Collab Capital Gestora de Recursos S.A. (“GESTORA”) formaliza o seu compromisso com a proteção de Informações Sigilosas e Segurança Cibernética (cyber security), conforme definição adiante, devendo ser cumprida por todos os Colaboradores.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Sigilosas.

2. OBJETIVO

Esta Política visa proteger as Informações Sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e audibilidade das mesmas, conforme art. 4º, §8º, da Resolução CVM n.º 021/2021, assim como à Lei 13.709, de agosto de 2018 (“Lei Geral de Proteção de Dados”), com intuito aprimorar a segurança cibernética da Gestora, nos termos do Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros, seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA.

Geralmente, nenhuma informação sigilosa deve ser divulgada, dentro ou fora da Gestora, a quem não necessite ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação, independentemente de ser considerada Informação Sigilosa, seja sobre a Gestora, relativa às suas atividades, aos seus sócios, Fundos e Clientes dentre outras, ou obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza da maneira e conforme previstos nos documentos internos da Gestora.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização prévia do Diretor de Gestão de Riscos.

3. APLICAÇÃO

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Sigilosas e dos Ativos disponibilizados pela Gestora ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Gestora, sendo de responsabilidade individual e coletiva o seu cumprimento.

4. RESPONSABILIDADES NA GESTÃO DA POLÍTICA

Cabe a todos os Colaboradores

- Cumprir fielmente esta Política;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Sigilosas;
- Proteger Informações Sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Gestora;
- Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela Gestora;
- Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Sigilosas;
- Comunicar imediatamente a Área de Gestão de Riscos sobre qualquer descumprimento ou violação desta Política.

5. CONCEITOS E PRINCÍPIOS

Todas as Informações Sigilosas constituem ativos de valor para a Gestora, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Gestora, Clientes, Fundos e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve ser prioridade constante da Gestora, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Gestora. Assim, por princípio, a guarda e segurança das Informações Sigilosas deve abranger três aspectos básicos, destacados a seguir:

Confidencialidade: Somente pessoas devidamente autorizadas pela Gestora devem ter acesso às Informações Sigilosas;

Integridade: Somente alterações, supressões e adições autorizadas pela Gestora devem ser realizadas às Informações Sigilosas;

Disponibilidade: As Informações Sigilosas devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento ao Guia Anbima de Segurança Cibernética, a Gestora possui cinco pilares principais no seu programa de segurança cibernética:

i. Identificação e avaliação de riscos (*risk assessment*);
ii. Ações de prevenção e proteção;
iii. Monitoramento e testes;
iv. Plano de resposta.

A implantação e monitoramento da capacidade da Gestora para atender a estes pilares deverá ser feito pelo Diretor de Gestão de Riscos. Também a fim de atingir os objetivos dispostos acima, cada segmento de atuação da Gestora terá suas próprias responsabilidades.

A Gestora deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação do Diretor de Gestão de Riscos promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Sigilosas, para que possam agir de maneira apropriada frente às situações que requeiram respostas.

6. MODELO ADOTADO

A Gestora optou por não manter time próprio dedicado à segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (instalações, substituições, configurações), verificações e manutenções periódicas.

Dessa mesma maneira, a Gestora não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética. Quando necessário, as matérias a esta relacionadas serão apresentadas pelo Diretor de Gestão de Riscos e tratadas no Comitê de Gestão de Riscos.

7. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

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

A Gestora deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta. O Código Anbima de Segurança Cibernética definiu que os ataques mais comuns de criminosos cibernéticos (cybercriminals) são os seguintes:

i. **Malware**

São softwares desenvolvidos para corromper computadores e redes:

- **vírus:** software que causa danos a máquina, rede, softwares e banco de dados;
- **cavalo de Troia:** aparece dentro de outro software e cria uma porta para a invasão do computador;
- **spyware**: software malicioso para coletar e monitorar o uso de informações;
- **ransomware:** software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

ii. **Engenharia Social**

São métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

- pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

- phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

- vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

- smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

- acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

iii. **Ataques de DDoS** (**Distributed Denial of Services**) **e botnets**

São ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.

No caso dos botnets, o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

iv. **Invasões** (**advanced persistent threats**)

São ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ações de prevenção e proteção

A Gestora adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e redes, em função da relevância para acesso à sede e à rede, incluindo aos servidores. A Gestora trabalha com o princípio de que a concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Para fins de manutenção das Informações Confidenciais, a Gestora recomenda que seus Colaboradores:
- bloqueiem o computador quando esse não estiver sendo utilizado;
- mantenham anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro;
- descartem materiais usados, destruindo-os fisicamente;
- jamais revelem a senha de acesso aos computadores ou sistemas eletrônicos, de preferência modificando-as periodicamente.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Gestora 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 Gestora conta com recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais. Da mesma maneira, monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

A Gestora realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

A Gestora controla as informações confidenciais reservadas ou privilegiadas a que tenham acesso os seus sócios, diretores, administradores, profissionais e terceiros contratados por meio de armazenamento em nuvem segura e com acesso restrito.

A Gestora realiza testes periódicos anuais de segurança para os sistemas de informações utilizados pela gestora, em especial para os mantidos em meio eletrônico e armazenados em nuvem.

As informações direcionadas para endereços eletrônicos e ambientes externos à gestora apresentam disclaimers de confidencialidade e segurança da informação.

A Gestora realiza treinamento anual de Cybersegurança e Proteção de Dados para os seus sócios, diretores, alta administração e profissionais que tenham acesso a informações confidenciais, reservadas ou privilegiadas e participem do processo de decisão de investimento.

Monitoramento e testes

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Gestora ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito a monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da Gestora, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Área de Gestão de Riscos e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Gestora, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Gestora possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira, deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados,

bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a Gestora realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, em linha, inclusive, com o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Gestora. Dentre as medidas, incluem-se, mas sem se limitar:

i. Verificação dos logs dos Colaboradores;

ii. Alteração periódica de senha de acesso dos Colaboradores;

iii. Segregação de acessos;

iv. Manutenção trimestral de todos os hardwares;

v. Atualização de todos softwares e sistemas de apoio e controle;

vi. Backup diário, realizado na nuvem.

Sem prejuízo dos testes realizados na forma do Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Gestora, a Gestora realiza simulações de ataques e respostas da Gestora que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Gestora, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da Gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

PLANO DE RESPOSTA

Havendo indícios ou suspeitas fundamentadas, a empresa contratada deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações confidenciais, reservadas, privilegiadas, sigilosas ou outras falhas de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Procedimentos Internos para tratar casos de vazamentos

Esta seção estabelece as regras para responder a um incidente. Cada incidente apresentará desafios únicos que exigirão discernimento e resolução pela equipe de Compliance e Riscos, destacado para cada caso.

i. Qualquer colaborador ou terceiro que suspeite ou observe um incidente de segurança, vazamento de dados, possível comprometimento do sistema ou atividade maliciosa deve contatar o Comitê de Compliance através do e-mail compliance@collabcap.com.br. O contato inicial deve conter uma descrição sobre o caso e um meio para contato imediato do representante do Comitê com a pessoa que está reportando o incidente.

O representante do Comitê para atendimento ao incidente será determinado obedecendo a seguinte ordem de prioridade:

i. Lucas Aragão - Diretor de Compliance e PLD-FT
ii. Fabrício Oliveira - Diretor de Investimentos
iii. Tiago André Piccoli – Diretor de Gestão de Riscos

Determinar se houve um incidente de segurança e a natureza e gravidade do incidente, considerando as seguintes questões e discutindo-as no Comitê de Compliance, documentando também qualquer tratamento inicial:

- Os dados comprometidos contêm informações sensíveis da gestora, seus clientes, parceiros e/ou fornecedores?
- Existe a chance de ser necessário envolver mantenedores externos da lei (polícia, reguladores, promotoria etc.)?
- Existe o requisito ou o desejo de se realizar uma análise forense do comprometimento dos dados ou dos sistemas envolvidos?
- Se a resposta for “sim” para qualquer uma das perguntas acima, coordene imediatamente as ações a serem tomadas com o Comitê de Compliance e aplique as instruções abaixo conforme apropriado.
- Se a resposta for “não” para todas as perguntas acima, aplique as instruções abaixo conforme apropriado.
- Faça uma análise preliminar – isole o sistema ou os dados comprometidos, removendo os acessos aos mesmos através de dispositivos de rede e repositórios de dados. Caso precise de ajuda, entre em contato com a equipe de compliance e riscos o mais rápido possível. Determine o tipo de incidente de segurança – tente determinar a causa da atividade maliciosa e o nível de privilégio do sistema obtido pelo invasor e implemente as medidas corretivas apropriadas.

Se um sistema estiver comprometido:

i. Desabilite quaisquer contas comprometidas e encerre todos os processos nos quais essas contas sejam proprietárias;
ii. Compile uma lista de endereços IP envolvidos no incidente, incluindo entradas de log, se possível, e encaminhe os dados para o Comitê de Compliance;
iii. Determine os usuários que precisam alterar suas senhas devido ao comprometimento, bem como se eles possuem ou não contas em outros sistemas onde as mesmas credenciais são utilizadas, e notifique a área de Infraestrutura sobre essa necessidade e os sistemas envolvidos.

- Infraestrutura deve acompanhar a mudança da senha dos envolvidos após a notificação através do monitoramento do hash NTLM de suas contas – ou equivalente, como o arquivo etc./shadow.
- Infraestrutura deve considerar a possibilidade – e a probabilidade – de o atacante ou invasor ter acesso ao e-mail da conta comprometida e utilizar outra forma de contato.

Reconstitua o sistema e/ou dados e verifique se o acesso aos mesmos deve ser reestabelecido juntamente à área de compliance e riscos.

Segurança da Informação deve executar uma verificação de vulnerabilidade do sistema e/ou dados após o desbloqueio deles para identificar quaisquer problemas de segurança não resolvidos que possam ser utilizados em futuros ataques.

Lições Aprendidas Pós-Incidente:

i. Realizar uma reunião com o time envolvido na resposta ao incidente em até 48 horas após a conclusão da resposta;

ii. Revisar a cronologia dos eventos documentados;

iii. Identificar o que deu errado e o que deu certo;

iv. Identificar as ameaças ou vulnerabilidades que foram exploradas e determinar se podem ser mitigadas;

v. Revisar se a detecção ou prevenção de intrusão estava em vigor, ativa e atualizada;

vi. Documentar as “lições aprendidas” e atribuir as atualizações apropriadas ao treinamento de Cybersegurança e Proteção de Dados.

Em caso de necessidade, poderá ser contratada empresa especializada para combater o evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de Compliance e Código de Ética e Conduta.

Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que sumariamente, constar no Relatório de Controles Internos.

8. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Adoção de comportamento seguro

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da Gestora e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

i. Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;

ii. Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;

iii. Todo tipo de acesso aos dados e informações da Gestora, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;

iv. Assuntos relacionados ao desempenho de atividades e funções na Gestora não devem ser discutidos em ambientes públicos ou em áreas expostas (meios de transporte, locais públicos, encontros sociais);

v. As senhas de acesso do Colaborador aos sistemas da Gestora são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;

vi. Os Colaboradores devem bloquear seus computadores sempre que se ausentar de suas estações de trabalho;

vii. Somente softwares homologados e previamente aprovados pela Gestora podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe de serviços de informática da Gestora;

viii. Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da Gestora;

ix. Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter informações

sigilosas. Portanto, não podem ser parciais ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;

x. O acesso remoto à rede, às informações sigilosas e sistemas da Gestora somente será permitido mediante autorização do Diretor de Gestão de Riscos, e desde que seja estritamente necessário para o desempenho das funções do Colaborador. O Colaborador será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas da Gestora;

xi. O Colaborador deve evitar realizar acesso remoto à rede da Gestora a partir de um dispositivo público, e, caso o faça, deverá limpar o cache e deletar todos os arquivos temporários;

xii. Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da Gestora sem a autorização prévia do superior hierárquico do Colaborador.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento a terceiros, bem como com conteúdo político ou outro que possa colocar a Gestora em risco.

A Gestora se reserva ao direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da Gestora e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

A Área de Gestão de Riscos implantará as medidas necessárias para realizar o monitoramento, bem como para a estabelecer as permissões de acesso aos documentos e arquivos da Gestora. Nesse sentido, o monitoramento poderá ser realizado pela Área de Gestão de Riscos mediante:

i. Gravação dos ramais telefônicos internos;
ii. Gravação em vídeo do ambiente da sede da Gestora;
iii. Registro de mensagens de e-mail;
iv. Registro de acesso à Internet;
v. Registro de acesso à rede interna;
vi. Registro de acesso à documentos e arquivos;
vii. Outros tipos de gravação e registros implantados pela Gestora.

Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Área de Gestão de Riscos e/ou por prestador de serviços externo. Apenas a Área de Gestão de Riscos poderá acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia do Diretor Responsável. O Diretor de Gestão de Riscos poderá contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhados pelos prestadores de serviços serão para uso exclusivo do Diretor de Gestão de Riscos.

Sempre que necessário será lavrado termo de monitoramento e acesso aos arquivos contendo registros e gravações.

Gestão de acesso a sistemas de informação e a outros ambientes lógicos

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela Gestora são monitorados, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da Gestora, através de monitoramento a ser efetuado pela Área de Gestão de Riscos.

Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da Gestora deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Gestão de Riscos.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

i. Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
ii. Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de
iii. cada Colaborador por suas ações e omissões;
Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de
iv. Segregação das Atividades;
v. Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Gestora, ou que tenham mudado de função, se for o caso;
vi. Revisão periódica das autorizações concedidas.

Utilização da internet
O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da Gestora, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

Websites na internet
O acesso a sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da Gestora.

Adicionalmente, a Área de Gestão de Riscos poderá ser informada sobre acessos e tentativas de acesso a determinados sites.

Ramais telefônicos

Os ramais telefônicos utilizados na sede da Gestora pelos Colaboradores da Área de Gestão e da Área Comercial são gravados, e o conteúdo das conversas são armazenados em arquivos nos servidores da Gestora. Conforme já esclarecido anteriormente, a Área de Gestão de Riscos possui livre acesso às gravações com o propósito de verificação de conteúdo.

Ao término da verificação, a Área de Gestão de Riscos emitirá termo de monitoramento, nos termos do Anexo I, informando o arquivo acessado, a data do acesso e se foram identificados indícios que possam indicar eventual infração ao disposto nesta Política, e nos demais documentos internos da Gestora.

Mensagens instantâneas

A comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos particulares deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da Gestora, mas não está proibida.

A GESTORA reconhece que, em determinadas situações, as mensagens instantâneas podem ser uma valiosa fonte de informação e um método eficiente de comunicação. Portanto, permite que os Colaboradores utilizem o recurso de mensagens instantâneas para comunicações relacionadas às suas atividades, desde que sejam enviadas e recebidas exclusivamente através da plataforma designada pela Gestora para tais comunicações.

Utilização e conexão de equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Gestora.

A utilização de equipamentos pessoais por terceiros nas instalações da Gestora e a conexão destes na rede interna e à Internet requer autorização prévia e expressa da Área de Gestão de Riscos. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

A conexão de dispositivos móveis de armazenamento (USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Área de Gestão de Riscos.

Acesso de terceiros

O acesso de terceiros aos arquivos e sistemas da Gestora será possível, na forma definida pelo Diretor de Gestão de Riscos, mas deve sempre ser precedido da assinatura de um contrato de confidencialidade que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à Gestora, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

9. ENDEREÇO ELETRÔNICO

Eventuais comunicações para a Área de Gestão Compliance e Riscos devem ser enviadas para: compliance@collabcap.com.br

10. RECURSOS COMPUTACIONAIS

A Gestora utiliza um conjunto de softwares na nuvem para desempenho de suas atividades, além de recursos computacionais compatíveis com o nível de complexidade da operação.

DESCRIÇÃO DA INFRAESTRUTURA

O ambiente físico da Gestora é composto por salas de trabalho, havendo total segregação das atividades de gestão de carteiras das demais atividades da empresa. Tanto o ambiente da área de compliance e riscos, quanto da área de gestão de carteiras possuem acesso controlado.

A área de Telecomunicações da GESTORA preocupa-se em prover meios alternativos de contingência para sua estrutura central da rede de dados, com roteadores e telefones IP com gravação em nuvem.

A Rede de Dados é estruturada com conexão à Internet por meio de um firewall de última geração (NGFW). O acesso principal é realizado através de um link de 1 Gbps, com uma contingência robusta fornecida por um link de backup de fibra ótica redundante e suporte adicional de um roteador 5G de alta capacidade.

Todos os ativos e arquivos críticos estão localizados em provedor externo e contratados em regime de CLOUD COMPUTING.

Outros sistemas contratados

Para controle de ativos e passivos dos fundos, bem como para a gestão de Riscos de Mercado e de Liquidez, é utilizado sistemas e plataformas compatíveis com o nível de complexidade da operação.

11. REVISÕES E ATUALIZAÇÕES

Esta Política será revisada ao menos uma vez anualmente. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

Esta Política será revisada ao menos uma vez anualmente. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

12. CONSIDERAÇÕES FINAIS

A presente política está em constante evolução, concebida com o objetivo primordial de fortalecer os mecanismos de segurança da informação e segurança cibernética. Sua importância transcende o âmbito institucional, pois está intrinsecamente ligada à salvaguarda da integridade do sistema financeiro e à contenção de atividades criminosas. Este é estabelecido sobre os pilares da conformidade estrita com as normas regulatórias vigentes e da adesão irrestrita às diretrizes estabelecidas pelos órgãos autorreguladores competentes.

CONTROLE E REVISÃO

Controle e Revisão de Informações Gerais		
Aprovado por:	**Data de Aprovação:**	**Alteração**
Diretor de Gestão de Riscos e Diretor de Compliance/PLD-FT	13/08/2026	Versão Inicial