POLÍTICA DE SEGURANÇA CIBERNÉTICA

SPN GESTÃO DE INVESTIMENTOS LTDA

Dez/2024

SUMÁRIO

1. INTRODUÇÃO

A presente Política estabelece as regras, procedimentos e controles de segurança cibernética da GESTORA, de acordo com o parágrafo único do artigo 13 do Código de Administração de Recursos de Terceiros da ANBIMA. Assim, deverá ser seguida por todos os Sócios, Colaboradores e Terceiros contratados, independentemente do nível hierárquico, função e do tipo vínculo, se empregatício, societário ou prestação de serviços.

A Política de Cibersegurança segue práticas de mercado, bem como está de acordo com as leis, regulamentação e autorregulamentação aplicáveis e melhores Práticas da ANBIMA – Guia de Cibersegurança ANBIMA 2021.

Além das questões de segurança cibernética, também aborda a questão da segurança da informação digital, de forma a satisfazer os requerimentos detalhados na política de segurança da informação, quando se trata de informação digital.

2. OBJETIVO

O objetivo das regras sobre segurança cibernética da **GESTORA** é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, reduzir a exposição a perdas ou danos decorrentes de falhas de cibersegurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da **GESTORA** devem assegurar:

- a integridade (garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais);
- a disponibilidade (garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário);
- a confidencialidade dos ativos de informação (garantia de que o acesso à informação seja obtido somente por pessoas autorizadas) da **GESTORA**, observadas as regras de confidencialidade constantes do Código de Ética da **GESTORA**; e

- O confinamento das informações confidenciais dentro do perímetro de segurança digital designado no tópico subsequente.

3. DEFINIÇÕES DO PERÍMETRO DE SEGURANÇA DIGITAL

3.1. AMBIENTE SEGURO

I. Rede Local
   a. Servidores, estações de trabalho, equipamentos de rede e de segurança digital localizados no escritório da **GESTORA**;

II. Rede Virtual
   a. Servidores virtuais, estação de trabalho virtuais, dispositivos de armazenamento de arquivos digitais virtuais, localizados em um parceiro provedor de serviços de nuvem pública;

III. Aplicativos móveis
   a. Aplicativos para acesso de informações da **GESTORA** que poderão estar instalados em dispositivos móveis pessoais dos colaboradores;

IV. Aplicações Web para divulgação de informação
   a. Deverá ser utilizado acesso autenticado por usuário e senha para garantir que apenas os colaboradores terão acesso a essas informações

V. Servidores das contrapartes para troca de informações
   a. Para troca de mensagens, os servidores das contrapartes serão considerados parte da área de segurança digital. Tais servidores deverão ser catalogados e acessados através de um canal seguro.

3.2. FRONTEIRA DO PERÍMETRO DE SEGURANÇA

I. E-mail corporativo
   a. Rodando na rede local, rede virtual ou aplicativos móveis. Constitui uma fronteira de informação importante. Será monitorada e caso uma informação confidencial cruze essa fronteira, o Diretor de Compliance poderá tomar as medidas cabíveis referentes à vazamento de dados sigilosos.

II. Internet
    a. Acesso à internet pela rede local ou pela rede virtual. Aplicativos móveis dentro do perímetro não poderão acessar internet.
    b. Acesso deverá ser realizado por meio dos sistemas de comunicação oficiais da gestora, como os sistemas "suíte" do Microsoft 365.
    c. A GESTORA não bloqueia o acesso de nenhum Sócio ou Colaborador a sites de mensagens instantâneas e/ou redes sociais. Entretanto, orienta, fortemente, que o compartilhamento de dados e informações da Gestora seja realizado através dos canais de comunicação oficiais, como e-mail corporativo e teams. Tal orientação é reforçada nos treinamentos anuais
    d. Conexões de serviços de mensageria (por exemplo envio de trades de forma automatizada). Nessa modalidade deverá ser utilizada uma forma segura para trocar informação, por exemplo:
        - Canal VPN criptografado
        - Conexão SSL com protocolo TLS 1.2

III. Portas de acesso na estação de trabalho
    a. Leitores de CD ou DVD, Bluetooth, deverão ser desabilitados.

IV. Acesso à internet das estações de trabalho é realizado por via Proxy, por meio de um certificado gerado pelo Firewall.

V. Acesso via Remote Desktop para as estações de trabalho virtuais que estarão na nuvem
    a. Cada colaborador receberá um certificado que poderá ser utilizado para conexão de qualquer computador pessoal com conexão a internet às nossas estações de trabalho virtual.
    b. Nessa fronteira não poderá transitar nada além da informação de teclado, mouse, som e vídeo. Cópia de arquivos e texto não será possível.

3.3. AMBIENTE EXTERNO

I. Estação de trabalho conectadas na rede via VPN SSL.
II. Wi-Fi no ambiente da **GESTORA**
III. Outros aplicativos nos dispositivos móveis dos colaboradores
IV. Estações de trabalho pessoais
V. Qualquer site, servidor ou computador da internet não fora do item 2.1

O fluxo de informação que poderá atravessar o perímetro será apenas o de informações públicas. A equipe de segurança cibernética trabalhará em melhores esforços para mitigar a possibilidade de informações confidenciais cruzarem a fronteira.

Além disso, esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da **GESTORA** serão monitorados e gravados quando possível, com prévia informação, conforme previsto nas leis brasileiras.

A **GESTORA** exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4. RESPONSABILIDADES

4.1. RESPONSÁVEL PELA SEGURANÇA CIBERNÉTICA

A Diretoria **de Risco e Compliance** é o responsável por esta Política, sendo o principal responsável dentro da **GESTORA** para tratar e responder questões de segurança cibernética (“Responsável pela Segurança Cibernética”), bem como por implementar as regras e normas aqui estabelecidas e a sua revisão.

4.1.1. Principais atribuições do responsável pela segurança cibernética

Segue abaixo uma lista não exaustiva dos deveres e responsabilidades do Responsável pela Segurança Cibernética:

I. Testar a eficácia dos controles utilizados e informar ao Diretor de Risco e Compliance os riscos residuais.
II. Acordar com o Diretor de Risco e Compliance o nível de serviço que será prestado por terceiros contratados e os procedimentos de resposta aos incidentes.
III. Configurar os equipamentos e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança aqui estabelecidos, bem como definir e assegurar a segregação das funções administrativas a fim de restringir poderes de cada indivíduo e reduzir o

número de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

IV. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

V. Realizar auditorias periódicas de configurações técnicas e análise de riscos.

VI. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da GESTORA, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da **GESTORA**.

VII. Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da **GESTORA**.

VIII. Na ocorrência de qualquer incidente envolvendo risco cibernético, todo e qualquer Colaborador que perceba ou desconfie de tal incidente, deverá imediatamente informar o Responsável por Segurança Cibernética, que poderá convocar reunião do Comitê de Risco e Compliance.

4.2. ATRIBUIÇÃO DOS DEMAIS COLABORADORES

Caberá a todos os Colaboradores conhecer e adotar as disposições das Políticas de Confidencialidade e Segurança da Informação e da presente Política, e seus deveres e responsabilidades na manutenção da segurança corporativa. Deverão, ainda, proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados, assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades adequadas e buscar orientação do gestor imediato em caso de dúvidas, o qual recorrerá ao Responsável pela Segurança Cibernética, se for o caso.

Em caso de incidente que afete a segurança cibernética da **GESTORA**, o Colaborador deverá comunicar imediatamente ao Responsável pela Segurança Cibernética, diretamente ou por meio do canal apropriado. Em caso de descumprimento, ainda que involuntário, estará sujeito às sanções internas aplicáveis e a eventual responsabilização na forma da lei.

4.3. COMITÊ DE RISCO E COMPLIANCE

São Responsabilidades dos membros que compõem o Comitê:

I. Discutir, elaborar e aprovar as políticas, normas e procedimentos gerais relacionados à Segurança Cibernética;
II. Analisar os riscos identificados e aprovar os controles requeridos para o tratamento de tais riscos.
III. Apoiar a implantação de soluções para eliminação ou minimização dos riscos;
IV. Estabelecer uma relação consistente das estratégias de negócios e da Tecnologia da Informação com os aspectos de segurança;
V. Tratar todos os assuntos relacionados à segurança;
VI. Definir responsabilidades e autoridades relacionadas a ela;
VII. Definir necessidades para os negócios, no aspecto da Segurança Cibernética;
VIII. Comunicar aos componentes da estrutura organizacional quanto à importância de atender aos objetivos e requisitos legais relacionados;
IX. Aprovar as iniciativas para a melhoria contínua;
X. Prover recursos para a gestão, operação e monitoramento adequado;
XI. Garantir a contínua manutenção da Política de Segurança Cibernética.

5. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCO (RISK ASSESSMENT)

A **GESTORA** periodicamente deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido pela equipe de TI, pelo responsável por segurança cibernética e pelo diretor de Risco e Compliance da **GESTORA**, o qual deverá ser documentado com o fim de dar visibilidade à metodologia utilizada para avaliar e gerir as vulnerabilidades da **GESTORA**.

A **GESTORA** poderá contratar uma empresa terceirizada para tanto, caso o Responsável pela Segurança Cibernética julgue necessário e mediante aprovação do Diretor de Risco e Compliance.

Após a condução do referido processo, o Comitê de Risco e Compliance, junto com o responsável por segurança Cibernética, deverá discutir as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela **GESTORA**, considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade de o evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

I. Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
II. Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso (“Phishing”);
III. Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
IV. Vazamento de informações confidenciais.

Periodicamente, no mínimo anualmente, deverá a **GESTORA** revisar o processo de cibersegurança com o fim de estabelecer, manter e monitorar a estrutura de governança de cibersegurança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

6. SISTEMAS DE PROTEÇÃO DO AMBIENTE SEGURO

Será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação um colaborador da **GESTORA**, sendo que os usuários e senhas de cada Colaborador serão de sua responsabilidade. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

Com relação ao monitoramento e auditoria do ambiente, a **GESTORA** possui sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, aplicativos para dispositivos móveis, filmagem e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

A **GESTORA** estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é

responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

6.1. INFRAESTRUTURA

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do Responsável pela Segurança Cibernética, ou de quem este determinar. As áreas que necessitarem fazer testes deverão solicitá-los previamente ao Responsável pela Segurança Cibernética, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a equipe de TI mediante registro de chamado junto ao Responsável pela Segurança Cibernética.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

6.2. USO DE E-MAIL E MENSAGEM INSTANTÂNEA

O envio ou repasse por e-mail de material que contenha conteúdo reservado, confidencial, discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da GESTORA, inclusive que contenha fins políticos locais ou do país (propaganda política).

Os Colaboradores devem evitar conduzir suas atividades por meio de qualquer rede de comunicação não pré-aprovada pela GESTORA (p.ex., e-mail externo, mensagem instantânea ou mensagem de texto não fornecido pela GESTORA ao Colaborador). Todas as comunicações eletrônicas contempladas pelas exigências aplicáveis de manutenção de registro estão identificadas e preservadas da forma adequada;

Os Colaboradores devem observar que qualquer e-mail ou mensagem instantânea que constitua um registro sobre qualquer atividade, transação ou negócio da **GESTORA** deve ser mantido na forma de sua Política de Segurança da Informação e não podem usar uma plataforma não designada para enviar e receber mensagens instantâneas relacionadas as atividades de gestão.

6.3. USO DA INTERNET

Todas as regras atuais da **GESTORA** visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da Internet. Embora a conexão direta e permanente da rede corporativa com a Internet ofereça um grande potencial de benefícios, também propicia riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na Internet está sujeita a divulgação e auditoria. Portanto, a **GESTORA** reserva-se o direito de monitorar e registrar todos os acessos a ela, nos termos da legislação aplicável. Como mencionado, os equipamentos, tecnologia e serviços fornecidos para o acesso à Internet são de propriedade da **GESTORA**, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/Internet, estejam em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

Programas licenciados e instalados nos computadores, principalmente via Internet (“downloads”), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do Responsável pela Segurança Cibernética. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado poderá ser excluído pela equipe de TI. Os Colaboradores não poderão em hipótese alguma utilizar os recursos da **GESTORA** para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O download e a utilização de programas de jogos são proibidos.

6.4. SENHAS E IDENTIFICAÇÃO

Observado o disposto na Política de Confidencialidade e Segurança da Informação, o usuário e a senha para acesso aos dados contidos em todos os computadores, bem como

nos e-mails, devem ser conhecidos pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros. O Colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins.

Todos os dispositivos e aplicações de identificação utilizados na **GESTORA**, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a **GESTORA** e a legislação (cível e criminal).

6.4. CRIPTOGRAFIA

Todos os dispositivos utilizados na GESTORA devem estar criptografados. Os arquivos devem ser criptografados codificando os materiais do usuário em algoritmos para que a leitura desses arquivos só seja realizada com uma decodificação especial, liberada por meio de uma chave específica.

6.5. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA DE TERCEIROS

Os Colaboradores externos da **GESTORA**, dentre os quais os seus fornecedores, prestadores de serviços e parceiros, também podem representar uma fonte significativa de riscos de cibersegurança. A computação em nuvem pode ser considerada como uma forma de contratação de serviço de terceiros e, assim como as demais contratações de Colaboradores externos, envolve determinados riscos que devem ser levados em conta pela **GESTORA**, demandando certos cuidados proporcionais a esta identificação de ameaças.

7. GOVERNANÇA

O programa de segurança cibernética deve ser revisado periodicamente, no mínimo anualmente, mantendo sempre atualizadas suas avaliações de risco, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes.

Os grupos envolvidos com o programa devem manter-se atualizados com novas vulnerabilidades e ameaças identificadas que possam alterar a exposição da instituição aos riscos avaliados originalmente. Isso pode ser feito, entre outras formas, por meio de participação em grupos de compartilhamento de informações, ou via fornecedores especializados.

Deverão ser criados indicadores de desempenho (key performance indicators) para corroborar a conscientização e o envolvimento da alta administração.

Um treinamento sobre o programa de segurança cibernética deve ser realizado com a periodicidade anual. Ele deve incidir periodicamente sobre todos os colaboradores, além de haver um plano de treinamentos especiais para funcionários recém-contratados, no momento do *onboarding*.

Os treinamentos e as campanhas de conscientização devem ser intensificados para os funcionários que trabalham remotamente e para os funcionários que foram vítimas de incidente cibernético.

8. MONITORAMENTO E TESTES

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

Para garantir as regras mencionadas nesta Política, a GESTORA:

I. Mantém sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II. Mantém sistemas de prevenção e detecção de informações cruzando o perímetro de segurança digital;

Todo e qualquer arquivo salvo nos dispositivos (físicos ou virtuais) da **GESTORA** é de propriedade da **GESTORA**, portanto, passível de auditoria e monitoramento. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

Ademais, sempre que possível a GESTORA deverá realizar *pentests* (testes de invasão), assim como análises de vulnerabilidades no parque tecnológico da GESTORA, que deverão ser realizados por empresa técnica a ser contratada pela Diretoria de Risco e Compliance.

9. REVISÃO

A **GESTORA** manterá o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio do Programa previsto na Política de Treinamento e Reciclagem da **GESTORA**.

O Responsável pela Segurança Cibernética, em conjunto com o Comitê de Risco e Compliance, realizará a revisão e atualização desta Política periodicamente, no mínimo anualmente ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do responsável pela Segurança Cibernética.